knowledge17

WORK at LIGHTSPEED™

ServiceNow SecOps and GRC Roadmap

HAROLD BYUN
SR. DIRECTOR, PRODUCT MANAGEMENT
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Key Business Challenges
- Security Operations Roadmap
- GRC Roadmap

© 2017 ServiceNow All Rights Reserved

Speaker Introduction

NAME: Harold Byun

TITLE: Sr. Director, Product Management

FUNCTION: Head of product management for SecOps and GRC

COMPANY: ServiceNow

EXPERIENCE: 20+ years in security architecture and product

EXPERTISE: Security, Encryption, Behavioral Analytics

ACHIEVEMENTS: Heads up PM for the security business unit. Has worked on several market leading security products in their respective sectors

CURRENT PROJECTS: Security automation, vendor risk management launch, planning for next release

© 2017 ServiceNow All Rights Reserved

Session Overview



Objectives

- Review of the Key Features in Jakarta and Istanbul and roadmap preview for K



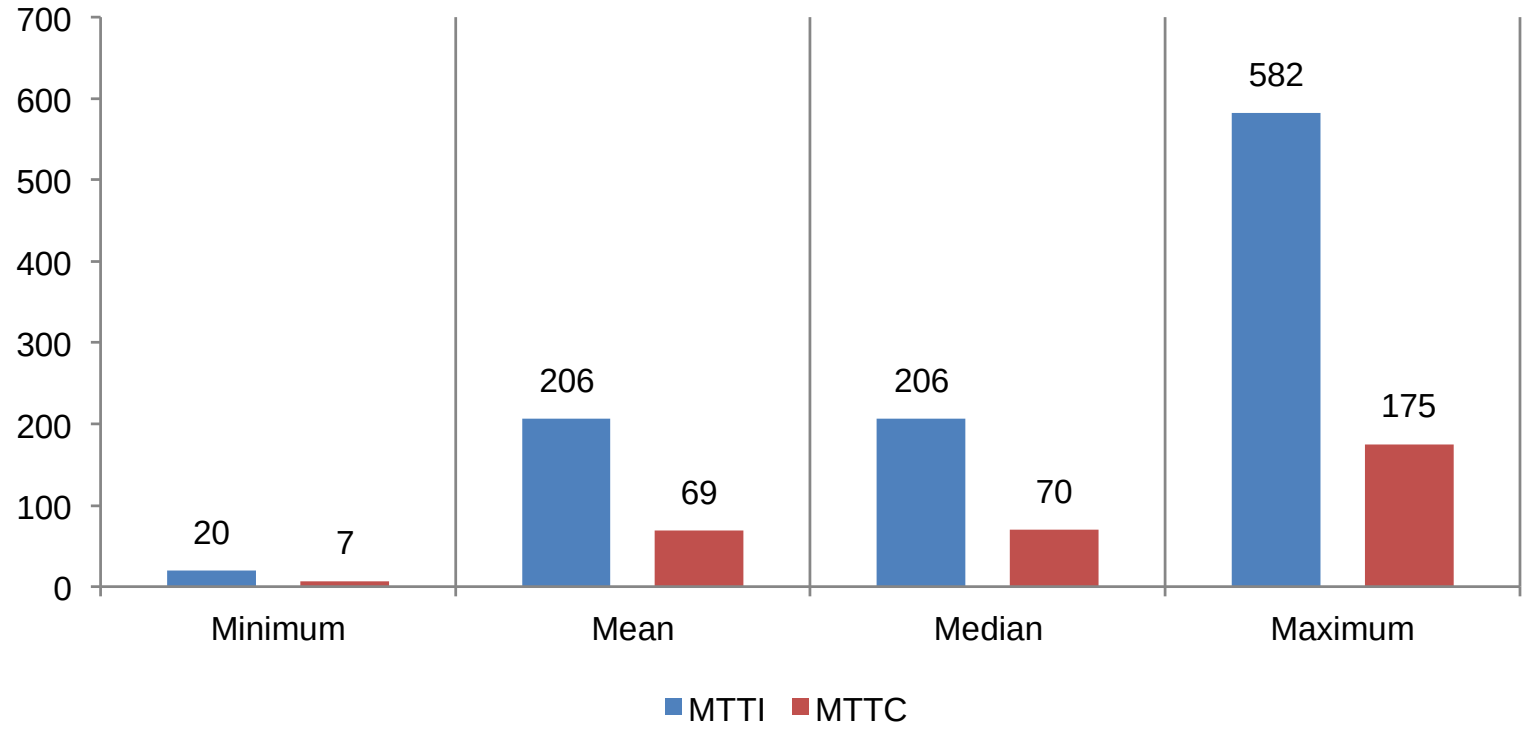
What You Will Learn

- Key features released in I and J releases
- Automation capabilities for SecOps
- Preview of Vendor Risk
- Overview of release plan for Kingston

© 2017 ServiceNow All Rights Reserved

Time to Containment is Key to Reducing Cost and Impact of Breach

Figure 17. Mean time to identify and contain data breach incidents (in days)
Consolidated view (n = 350)



ON AVERAGE, IT TOOK RESPONDENTS 206 days to spot a breach caused by a malicious attacker, and 69 DAYS TO CONTAIN IT.

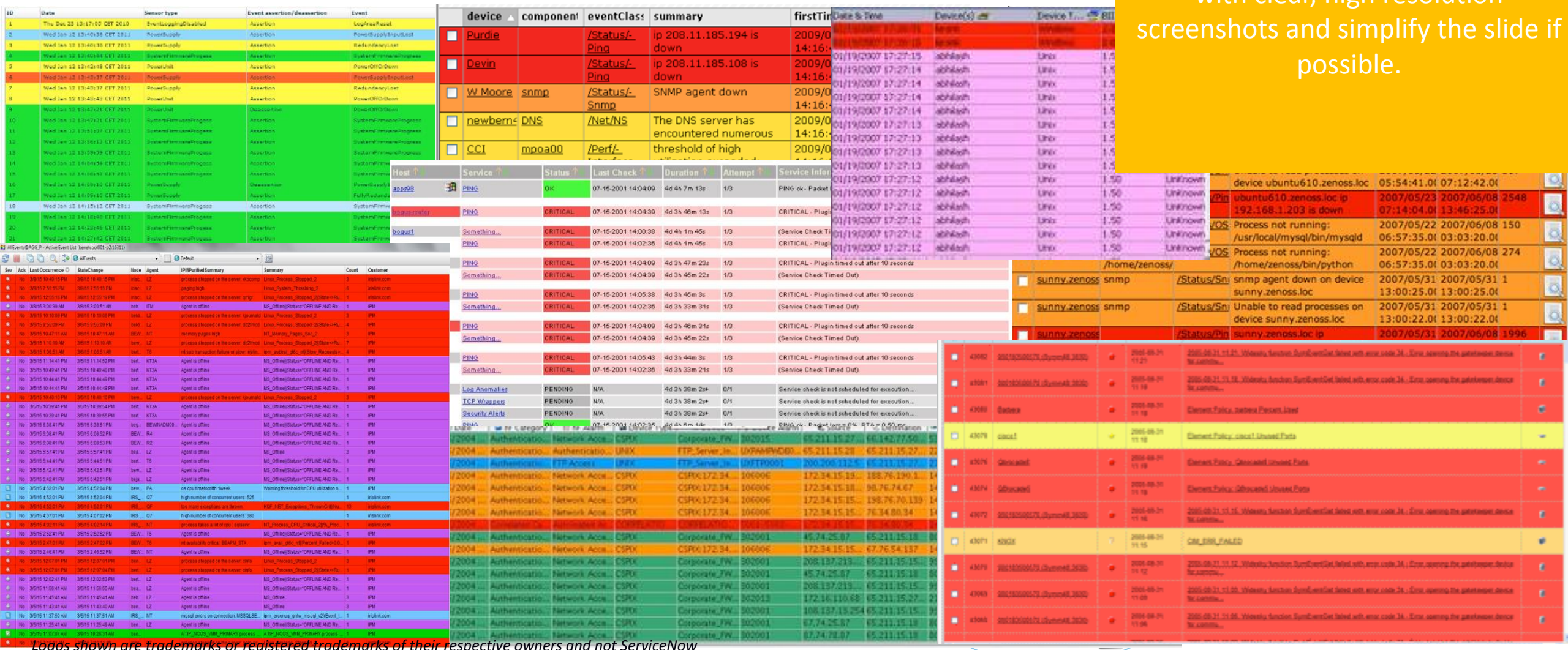
Source: Ponemon Institute 2015

Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

Why is Security Response Time Slow?

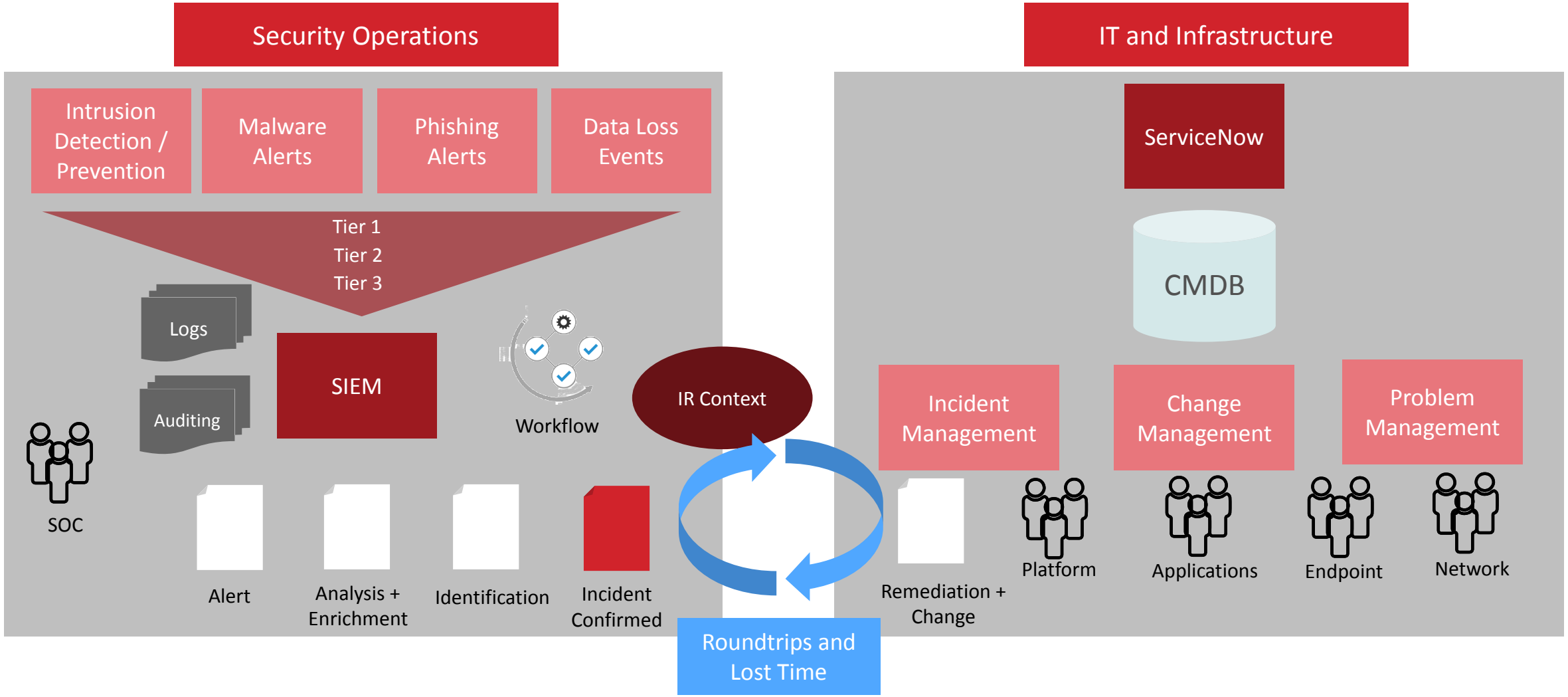
Please replace unclear screenshots with clear, high resolution screenshots and simplify the slide if possible.



Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

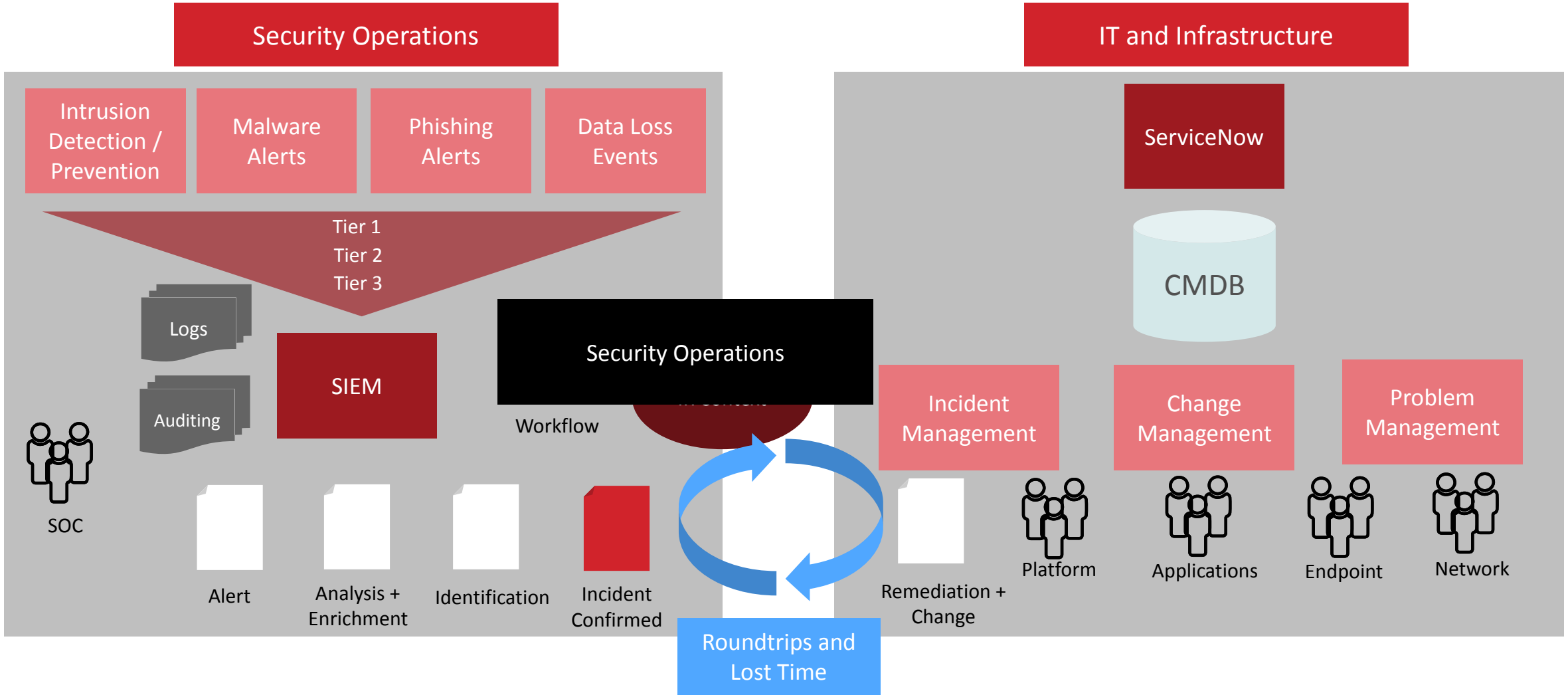
© 2017 ServiceNow All Rights Reserved

Current Operating Model



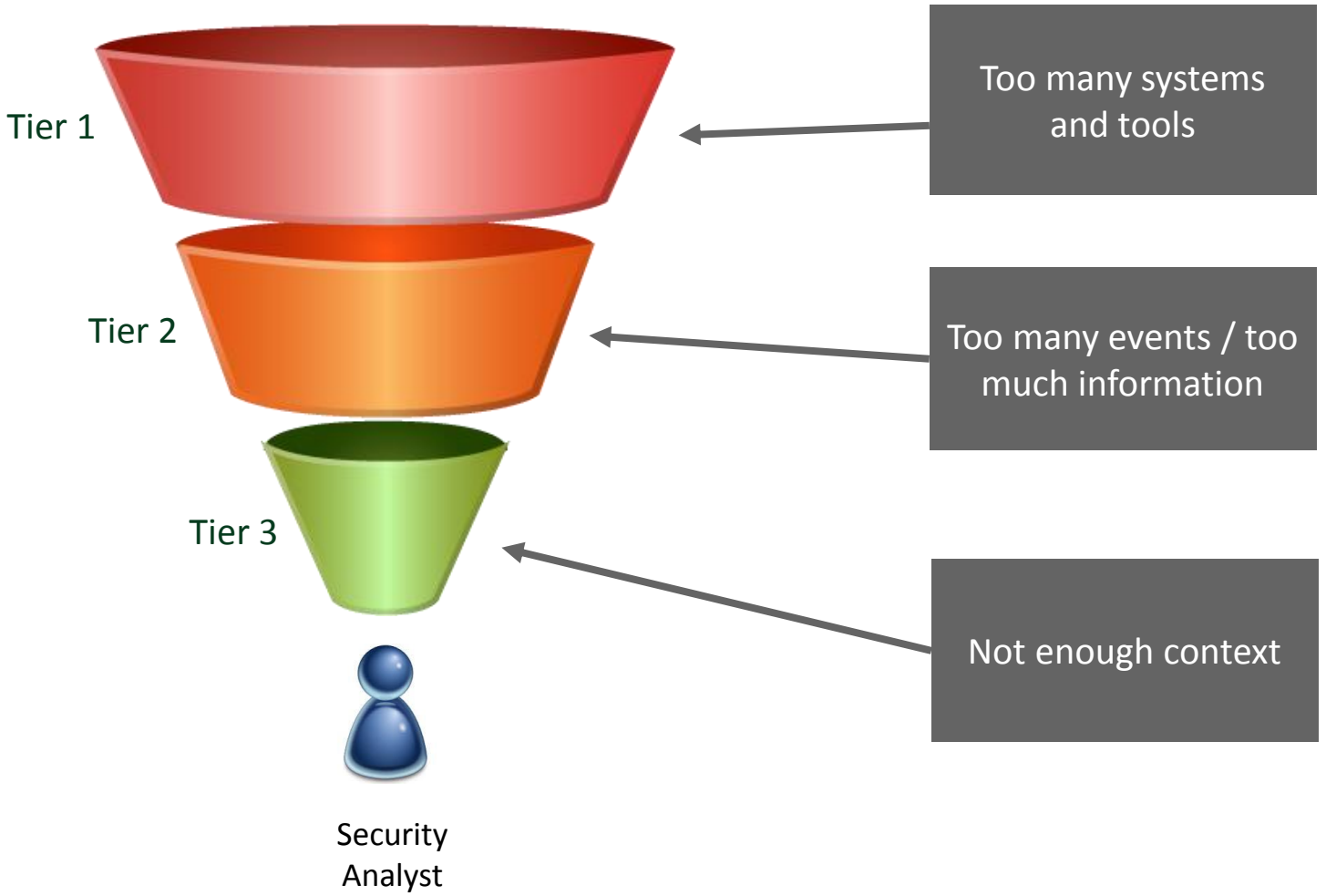
© 2017 ServiceNow All Rights Reserved

Alternate Operating Model



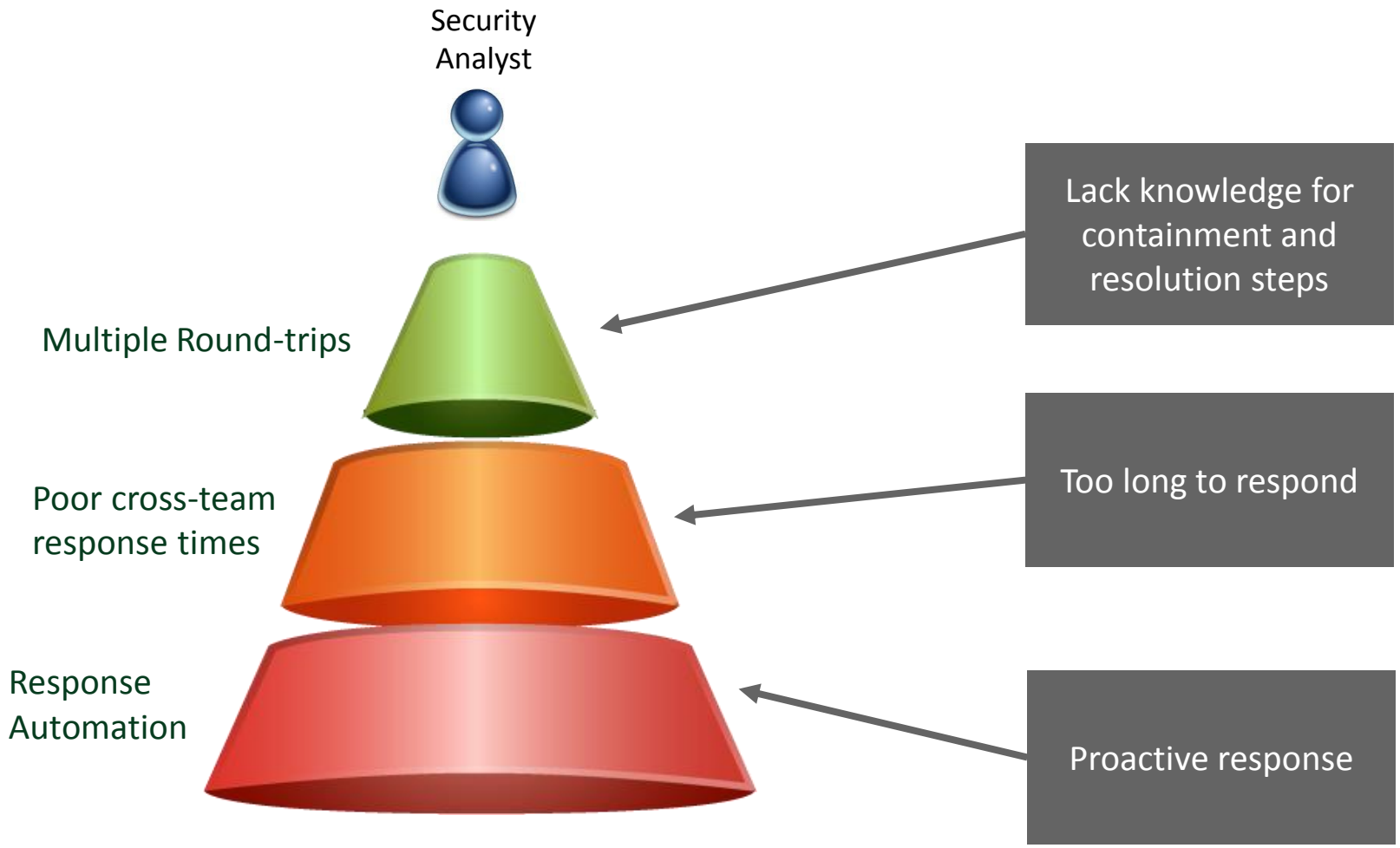
© 2017 ServiceNow All Rights Reserved

Security Response Optimization – Time to Identify/Detect



© 2017 ServiceNow All Rights Reserved

Security Response Optimization – Time to Contain



© 2017 ServiceNow All Rights Reserved

SecOps Key Themes

Accelerate Operationalization	• Enable "Go Lives" with zero PS in one day • Enhance usability for key personas
Ecosystem Expansion	• Build integrations for tier 1 vendors to support core operationalization • Enable rapid ecosystem expansion and automation use cases
Build a Security Intelligence Sharing Network	• Enable a security intelligence sharing network to create a barrier to entry • Deliver attack assessment and discovery capabilities
IR Automation and Orchestration	• Compress "Time to Identify" security incidents • Compress "Time to Contain" and remediation of incidents

© 2017 ServiceNow All Rights Reserved

Historical View to Date



Geneva (Dec ‘15)

Security Incident Response Core

- NIST Framework Support
- Severity Calculator
- ServiceWatch Integration
- Post Incident Review

Vulnerability Response Core

- Vulnerability Feed Support
- Nat’l Vulnerability DB Integration
- ServiceWatch Integration

Helsinki (May ’16)

Threat Intelligence

- IOC Support
- STIX and TAXII Support
- Loose Correlation on Threat

Accelerate Operationalization

- Updated Dashboards
- PA Plugin Support
- Simplified Email Parser

Ecosystem Expansion

- Splunk
- Qualys
- Tenable

Istanbul (Jan ’17)

IR Automation

- Automated data enrichment
- Threat intel lookups
- Initiate block on firewall

Accelerate Operationalization

- Critical Asset Identification
- Privileged Access ACLs
- Incident Dashboards

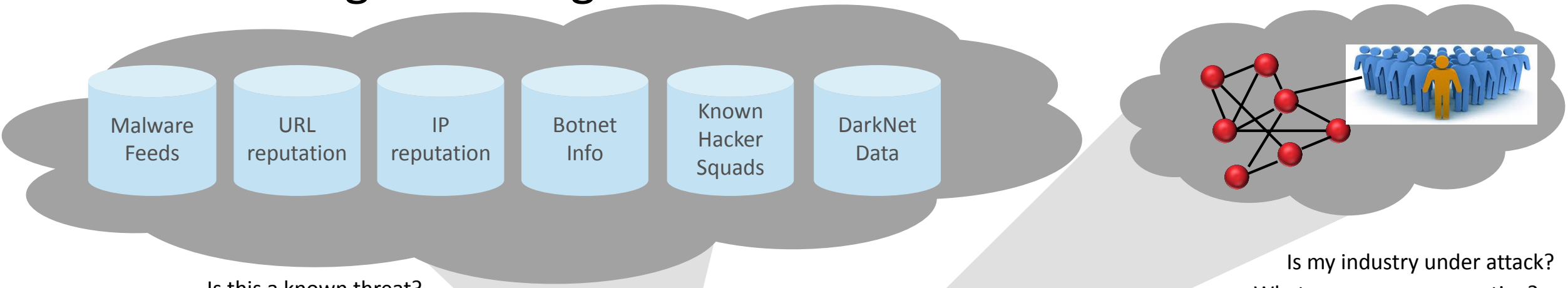
Ecosystem Expansion

- QRadar
- Tanium
- Palo Alto Networks
- Microsoft SCCM, WMI
- VirusTotal, MetaDefender

© 2017 ServiceNow All Rights Reserved

Threat Intelligence Integrations

Info Sharing and Analysis Communities (ISAC)



Is this a known threat?

Have we seen this before?

Where has it been seen?

What is the attack behavior?

Is my industry under attack?

What are my peers reporting?

What is the threat prevalance?

What is confidence rating from the community?

TAXII Profile Feed Exchange

Threat Intelligence

Security Incident Response

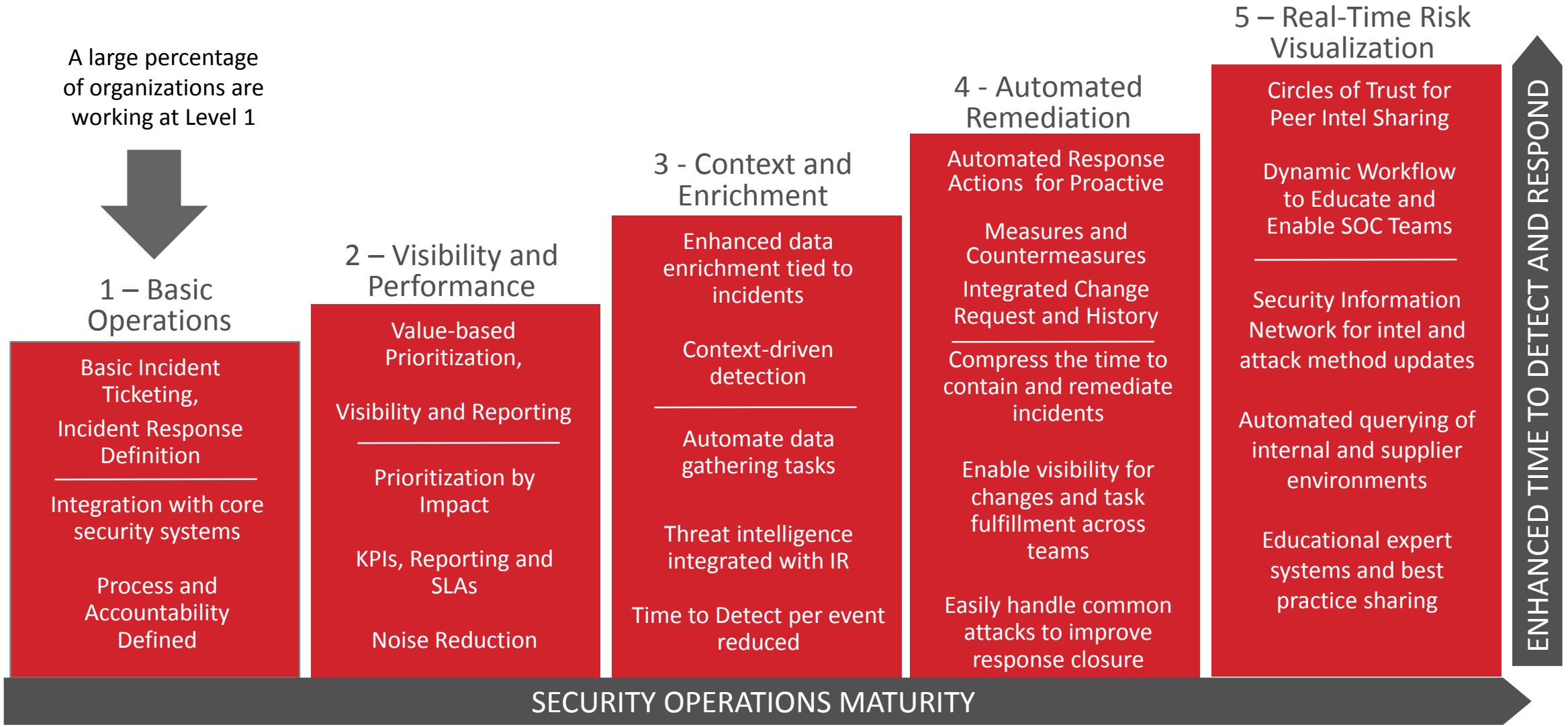
Vulnerability Response

ServiceNow Security Operations

ITSM Platform

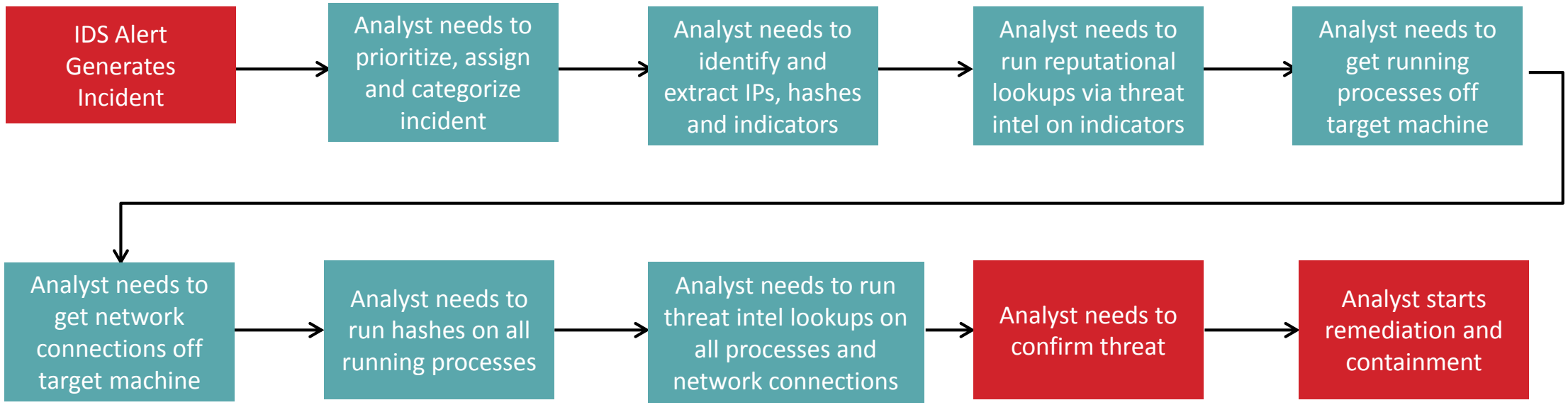
© 2017 ServiceNow All Rights Reserved

Security Operations Maturity Levels



© 2017 ServiceNow All Rights Reserved

Sample Response Workflow



*Note: Blue boxes indicate data enrichment activities

© 2017 ServiceNow All Rights Reserved

Security Operations Overview

servicenow®
securityoperations

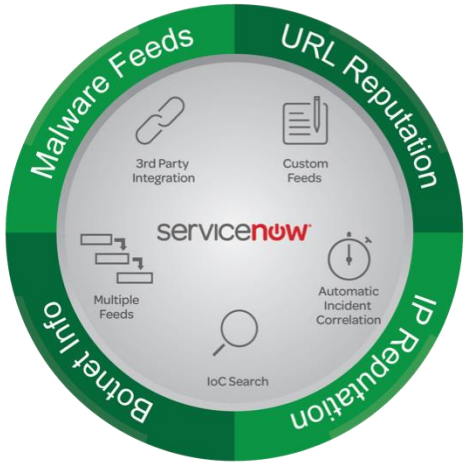
Security Incident Response



Vulnerability Response



Threat Intelligence



© 2017 ServiceNow All Rights Reserved

Security Operations and GRC Roadmap

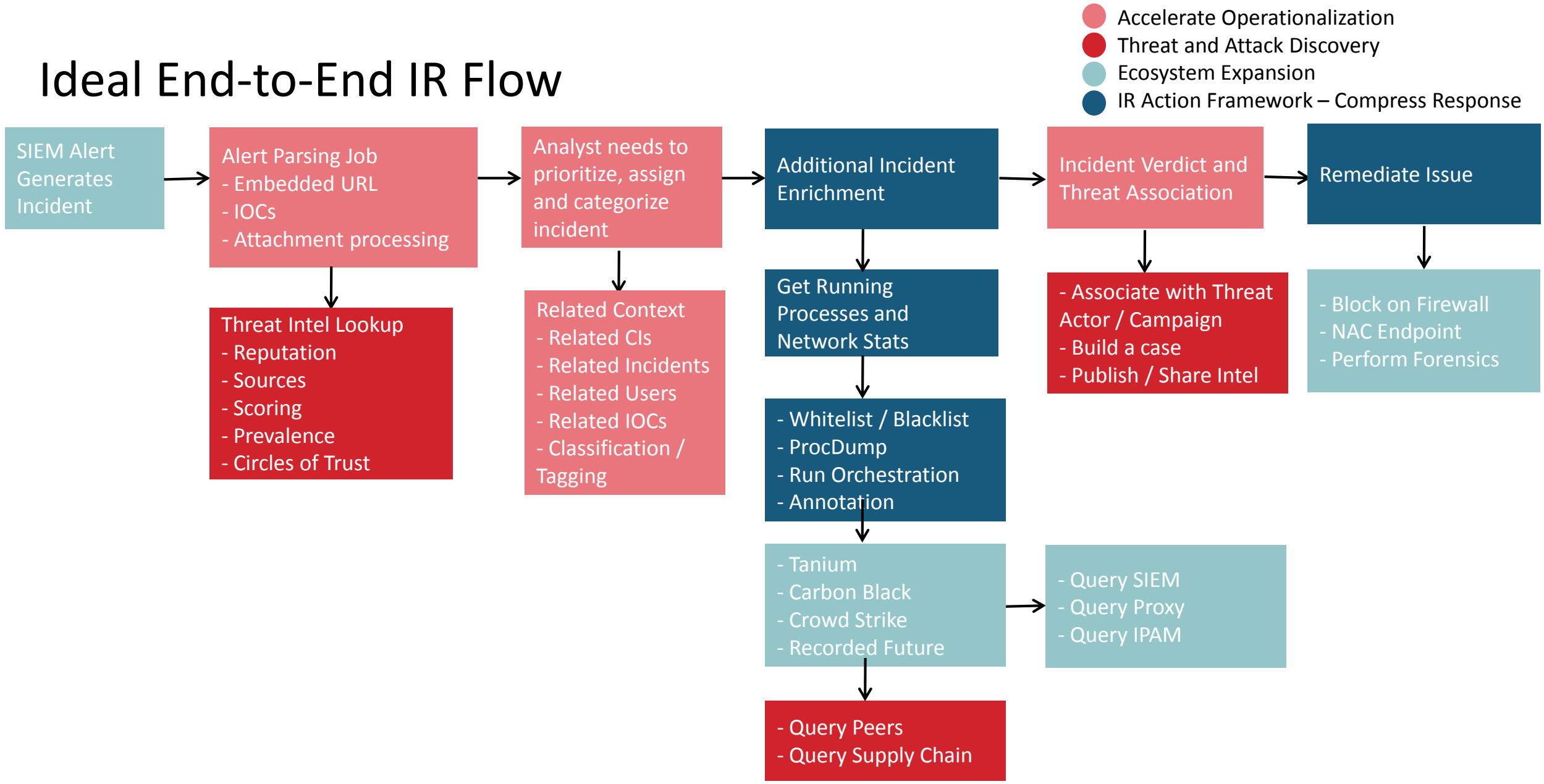
© 2017 ServiceNow All Rights Reserved

Goals for Jakarta

Enable IR Action Framework	• Improve automated data gathering and analysis, and investigations flows • Deliver additional orchestration capabilities
Deliver Threat and Attack Discovery Model	• Integrate BrightPoint Security functionality and intel sharing • Deliver case management and adversary tracking
Expand the Security Ecosystem	• Build key integrations to enable L1 maturity use cases and build a security ecosystem • Deliver in integrations API abstraction layer
Accelerate Operationalization	• Enhance customer onboarding and presentation of information • Metalayer for classification, grouping, permissions and remediation

© 2017 ServiceNow All Rights Reserved

Ideal End-to-End IR Flow

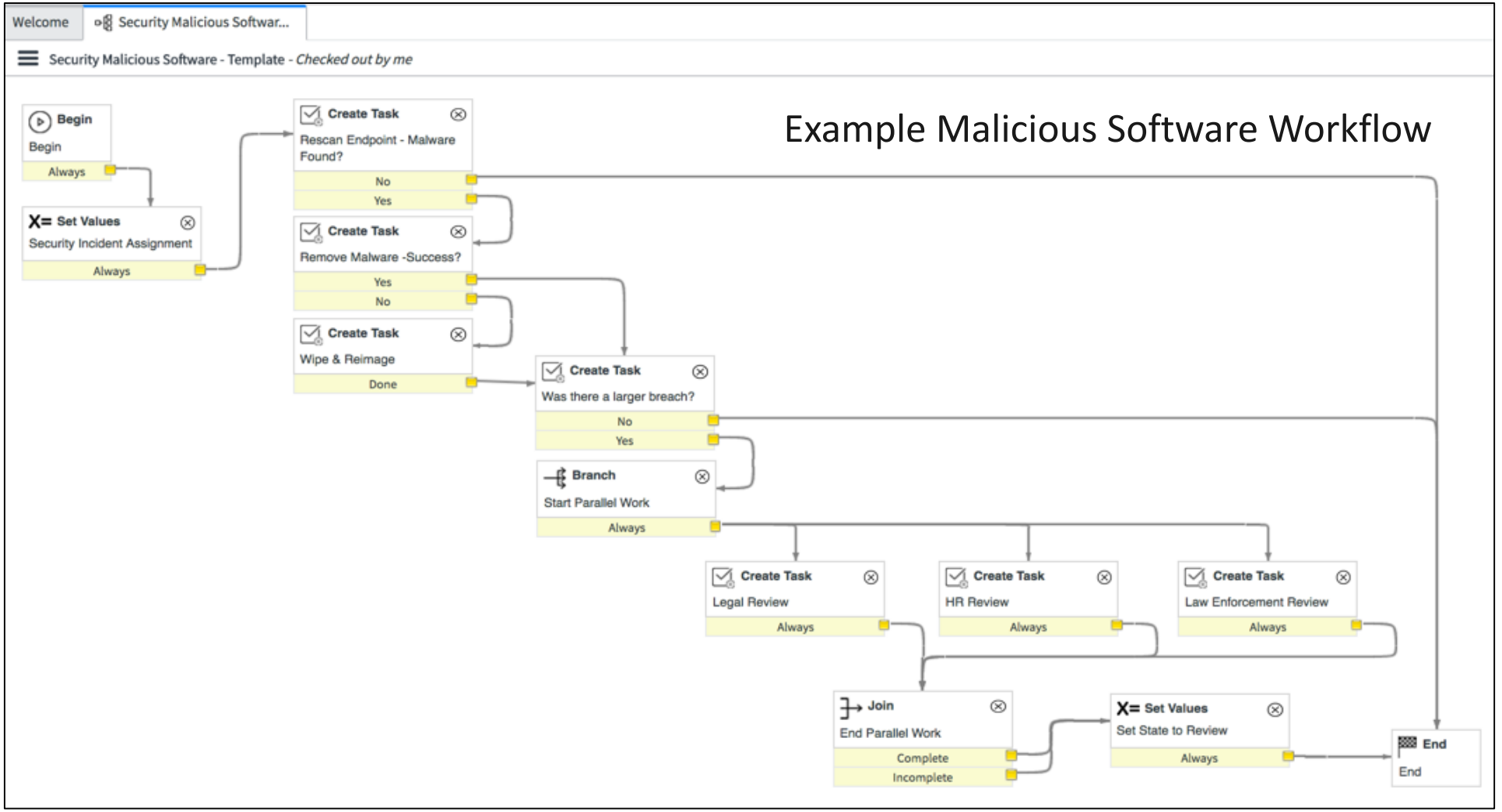


© 2017 ServiceNow All Rights Reserved

Accelerate Operationalization

© 2017 ServiceNow All Rights Reserved

Accelerate Operationalization – Out-of-the-Box Workflows

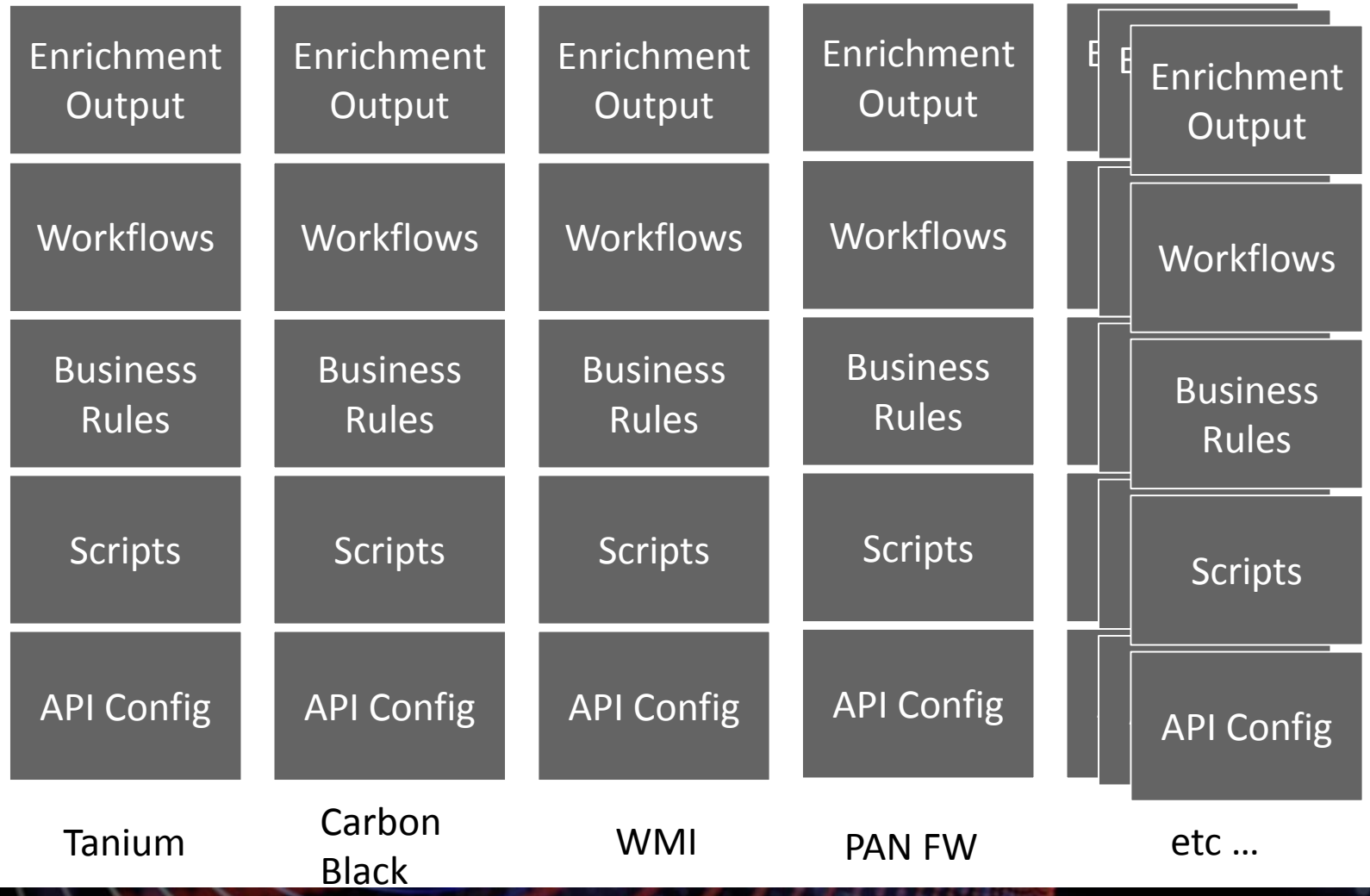


© 2017 ServiceNow All Rights Reserved

Expand Security Ecosystem

© 2017 ServiceNow All Rights Reserved

Existing Integration Development



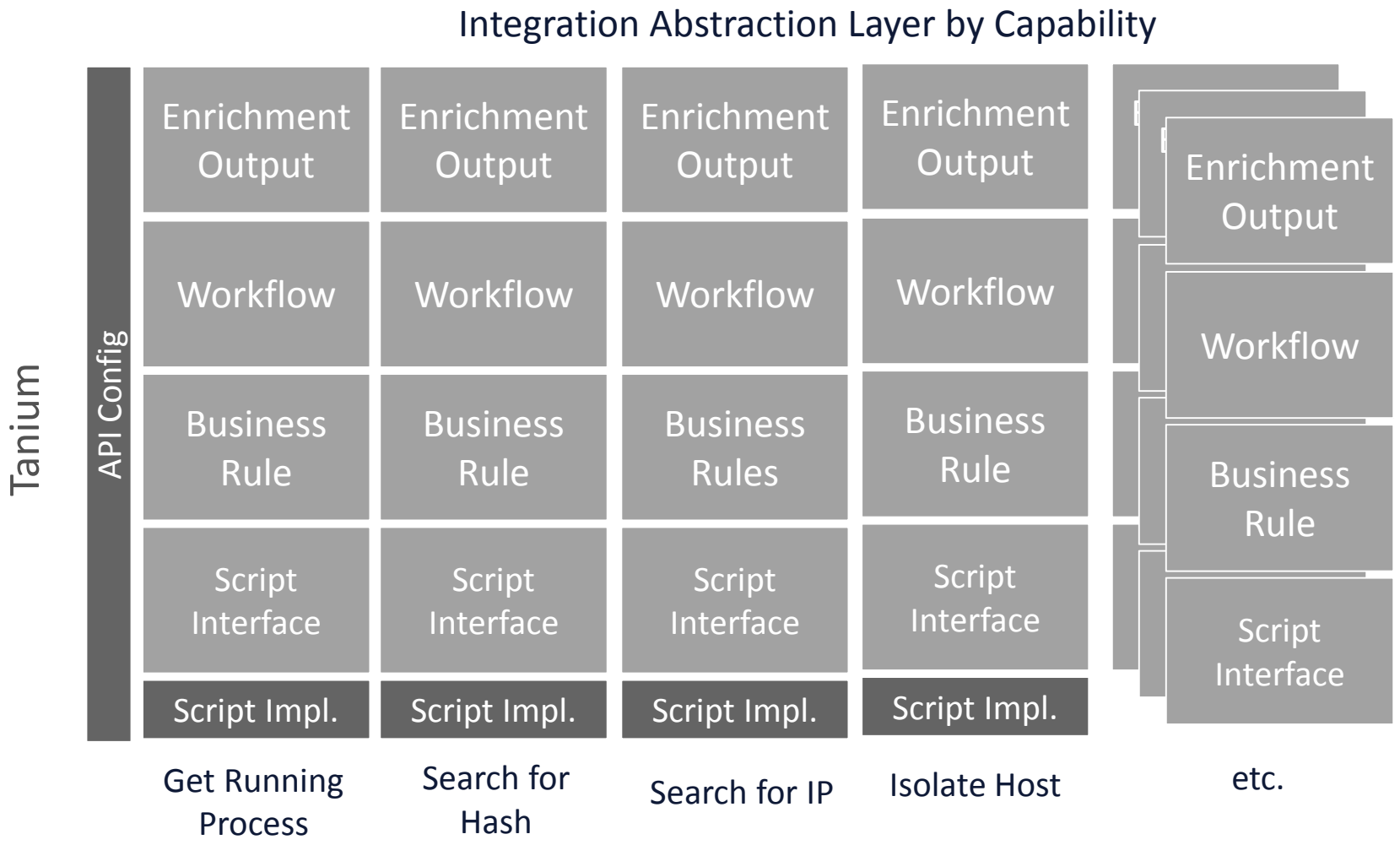
Key Challenges

- Development cost of each integration is high
- Inconsistent implementations and approaches
- Impacted by changes to core application suite in milestone releases

= dev cost

© 2017 ServiceNow All Rights Reserved

SecOps Integration Abstraction Layer



Key Benefits

- Development cost of each integration is lower
- Drives consistent implementations by capability
- Isolates integrations from changes to core applications in milestone releases
- Enables advanced playbooks dynamically link to integrations

= dev cost

© 2017 ServiceNow All Rights Reserved

Integration Abstraction Layer – How It Works

1. Integrations specify which capabilities they support
2. Abstracted workflows (e.g. “Get Running Processes”) dynamically ”link” to integrations that implement capabilities
3. Abstracted workflows for each capability can be leveraged in automated enrichment and larger playbooks

© 2017 ServiceNow All Rights Reserved

Jakarta Plan - Integrations

Early Maturity	3rd Party Development	Threat Community	Deployment Breadth
ADVANCED EMAIL PARSER	INTEGRATION ABSTRACTION LAYER	LOG QUERY DEFINITIONS	CROWDSTRIKE FALCON INTELLIGENCE
ARCSIGHT ESM	DEVELOPER GUIDE FOR VR	SPLUNK	CARBON BLACK
INTEL MCAFEE ESM	Additional Developer Guides	ArcSight Logger	MCAFEE EPO
LogRhythm		ElasticSearch	Exchange Online
			FireEye iSIGHT
			Anomali ThreatStream
			Recorded Future
			Checkpoint Firewall

PLANNED
Stretch

© 2017 ServiceNow All Rights Reserved

Security Ecosystem Partners

Vulnerability

- Qualys
- Rapid7
- Tenable Network Security
- Flexera Software
- Tripwire

Enforcement

- paloalto Networks
- Blue Coat
- Symantec
- McAfee
- Tanium
- Check Point Software Technologies Ltd.
- FireEye
- ForeScout
- Infoblox

SIEM

- splunk>
- Radar
- ArcSight
- LogRhythm — The Security Intelligence Company

Intelligence

- CrowdStrike
- Metascan
- ThreatConnect
- Carbon Black — Arm Your Endpoints
- iSIGHTPARTNERS
- virustotal
- Soltra — A DTCC and FS-ISAC Company
- Recorded Future
- cuckoo
- STIX

Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations – New Integrations

Vendor Product	SecOps Application	Use Cases	Integration Type
Malwarebytes	Security Incident	Email based incident creation & Powershell Script to kick-off a scan in Malwarebytes	Email/Script
Risk IQ – Passive Total	Threat Intelligence	Lookup observable- IP, Domain, File Hash	API
Cuckoo	Security Incident	Sending file/executables to Cuckoo and return results to SN	API
ThreatCrowd	Threat Intelligence	Look observables – Filehash, email, domain, url, AV detections	API
PhishTank	Threat Intelligence	Lookup suspected phishing site	API
GoogleSafeBrowsing	Threat Intelligence	Search URL against google list	API
Lastline	Security Incident	Incident creation via email	Email
VxStream	Threat Intelligence	Lookup hash, IP, Port, URL	API
Sumologic	Security Incident	Sightings Search	API
Shodan	Security Incident	Lookup IP's and URLs	API
IBM QRadar	Security Incident	Sightings Search	API
HPE Logger	Security Incident	Sightings Search	API
McAfee ESM	Security Incident	Sightings Search	API

Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations – New Integrations

Vendor Product	SecOps Application	Use Cases	Integration Type
Tripwire Enterprise	Security Incident	Bi-directional integation – open incidents in SN, perform lookups on TW Enterprise	Bi-Directional API
Anomoli	Threat Intelligence	Lookup Email, IP, URL	API
Kenna Security	Vulnerability Response	Pull scan data into ServiceNow and launch scans in Kenna from SN	API
Digital Shadows	Security Incident	Incident creation	API
CyberArk	Security Incident	Confirm SIR task/incident is validated before accessing credentials in CyberArk	API
Cylance	Security Incident	Consume alerts as security incidents or events	email
Phishme	Security Incident	Consume alerts as security incidents or events	email
Checkpoint & Passive Total	Security Incident	Workflow with block action	API
Slack	Security Incident	Multiple including creating channel for security incident, get transcripts	API
Reverse Whois	Security Incident	Lookup for enrichment	API
Tenable Nessus	Vulnerability Response	Request Scans	API
Splunk	Security Incident	Launch search in Splunk in context	API

Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

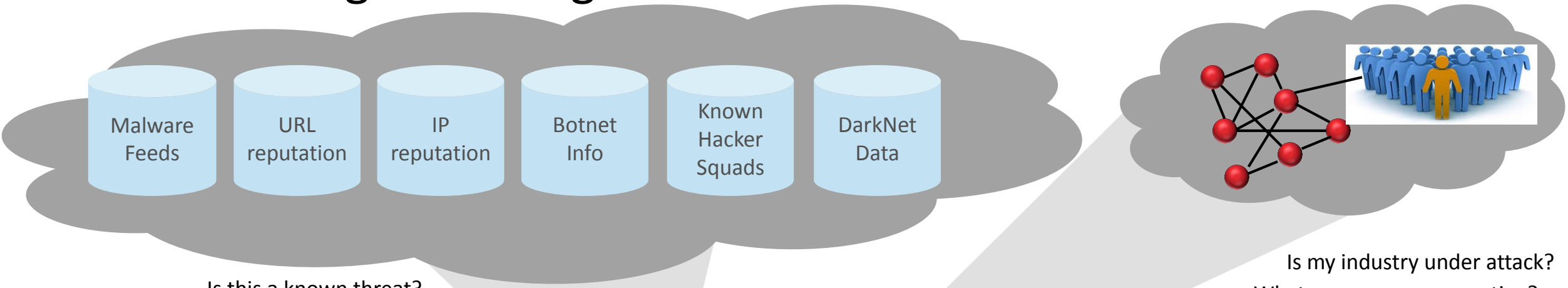
© 2017 ServiceNow All Rights Reserved

Threat and Attack Discovery Model

© 2017 ServiceNow All Rights Reserved

Threat Intelligence Integrations

Info Sharing and Analysis Communities (ISAC)



Is this a known threat?

Have we seen this before?

Where has it been seen?

What is the attack behavior?

Is my industry under attack?

What are my peers reporting?

What is the threat prevalance?

What is confidence rating from the community?

TAXII Profile Feed Exchange

Threat Intelligence

Security Incident Response

Vulnerability Response

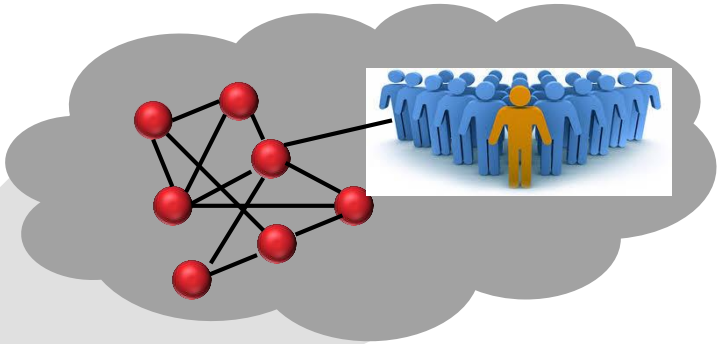
ServiceNow Security Operations

ITSM Platform

© 2017 ServiceNow All Rights Reserved

Threat Intelligence Integrations – Jakarta

Info Sharing and Analysis Communities (ISAC)



Malware Feeds

URL reputation

IP reputation

Botnet Info

Known Hacker Squads

DarkNet Data

Is this a known threat?

Have we seen this before?

Where has it been seen?

What is the attack behavior?

Is my industry under attack?

What are my peers reporting?

What is the threat prevalance?

What is confidence rating from the community?

SIEM / Data Lake

TAXII Profile Feed Exchange

Threat Intelligence

Security Incident Response

Vulnerability Response

ServiceNow Security Operations

ITSM Platform



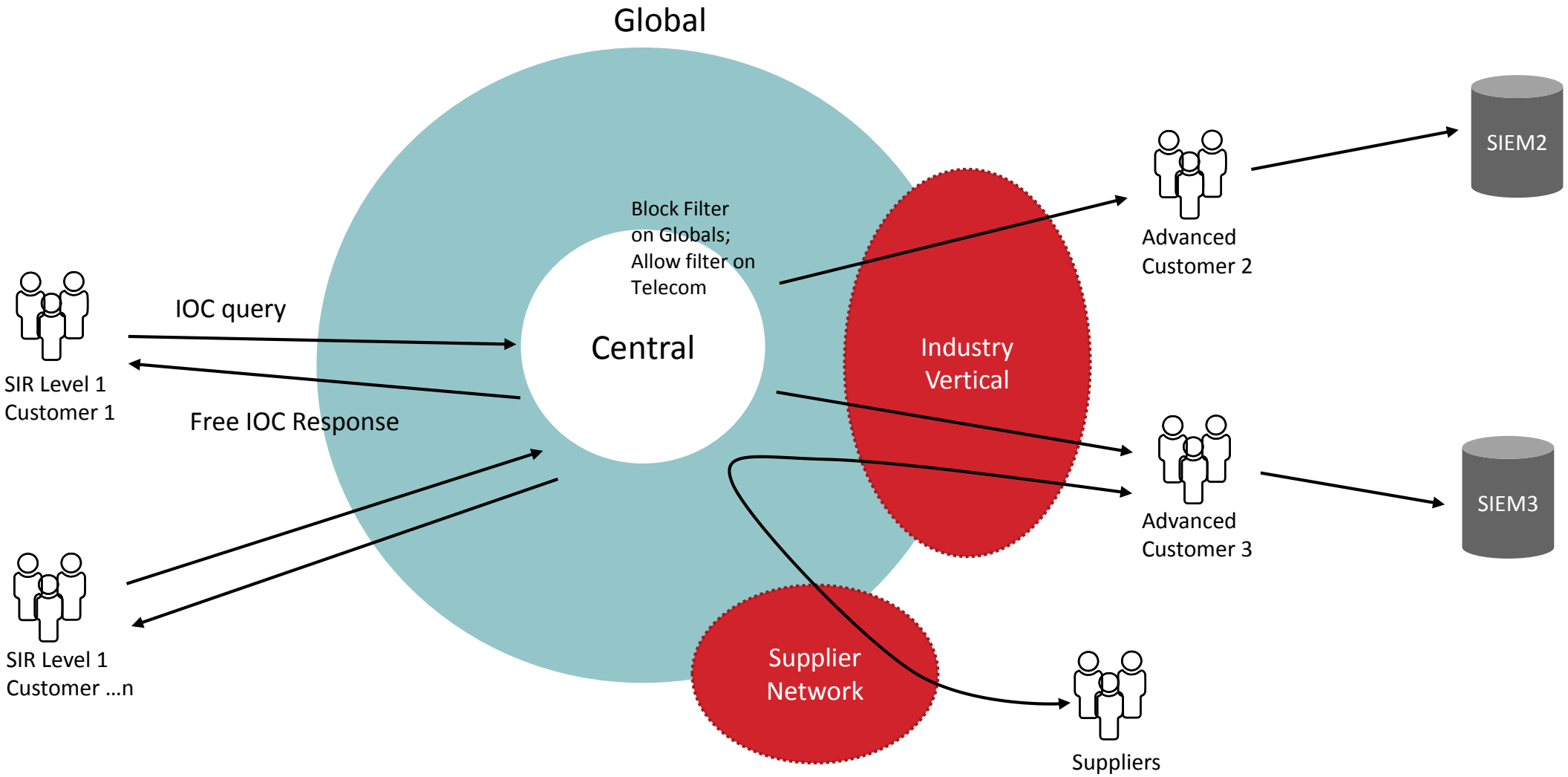
Trusted Communities



Supplier Network

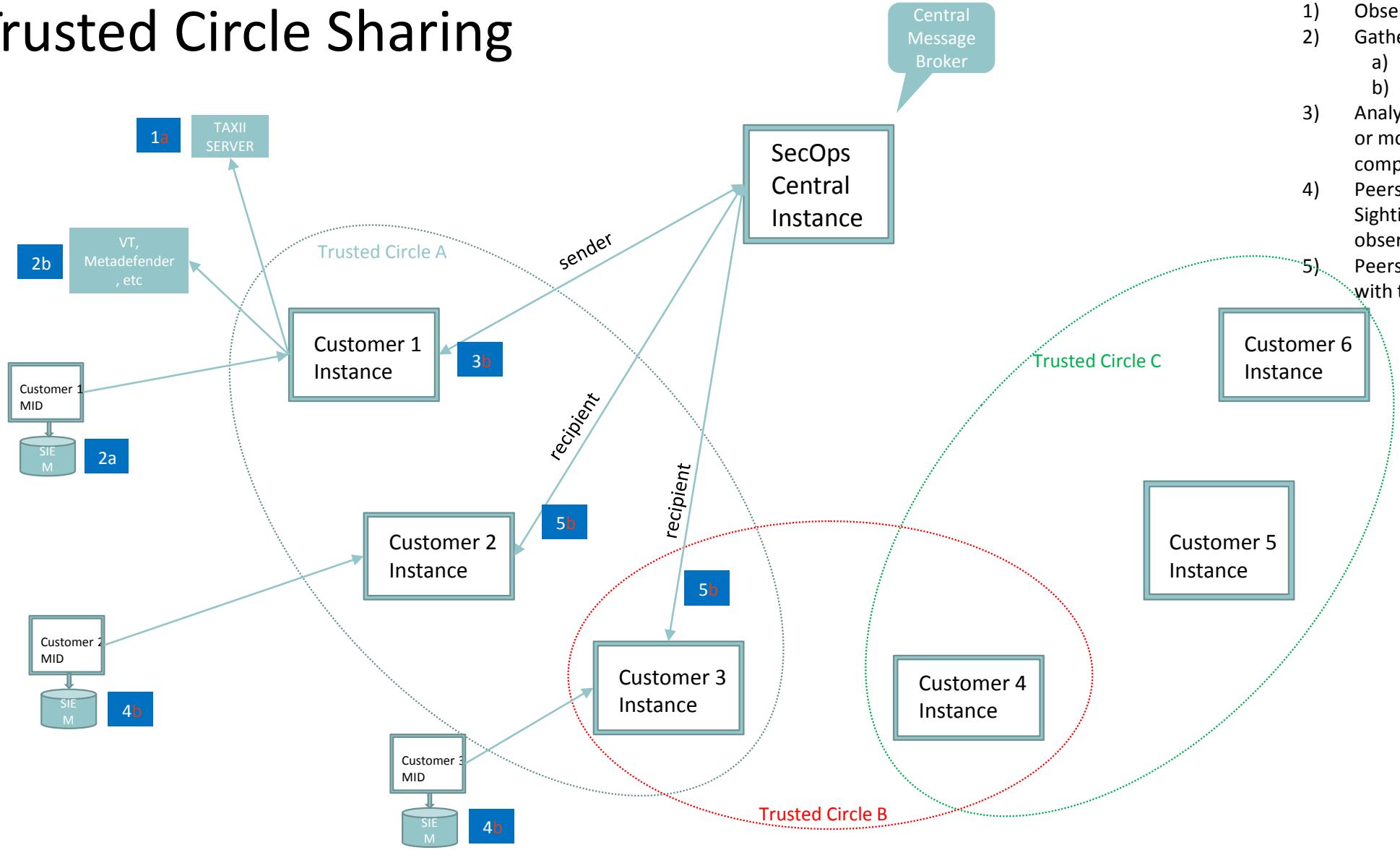
© 2017 ServiceNow All Rights Reserved

Threat Intel Sharing Circles



© 2017 ServiceNow All Rights Reserved

Trusted Circle Sharing

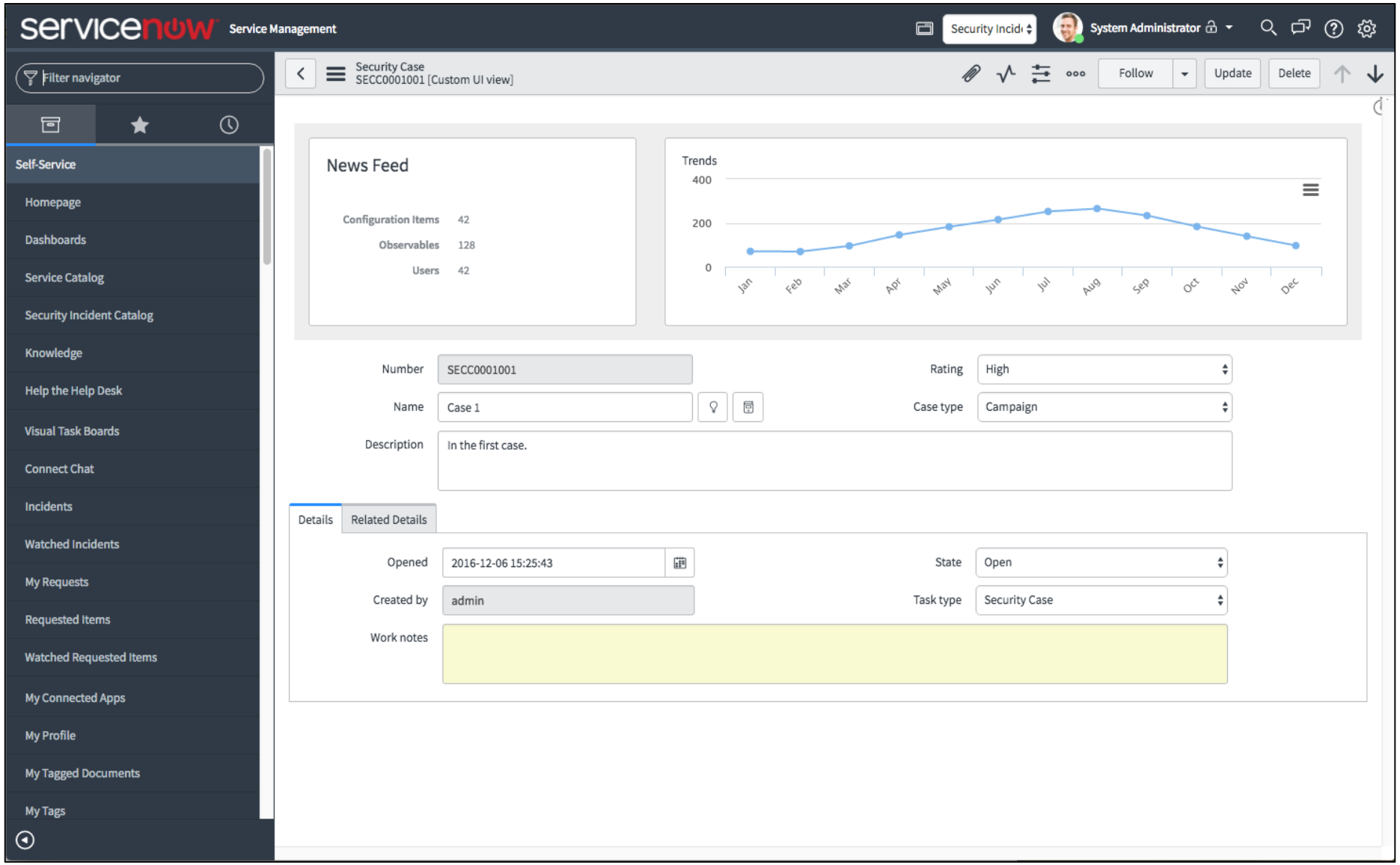


Example Flow

1) Observables (from somewhere)
2) Gather information about them.
   a) Local Sightings Search
   b) Get additional Enrichment
3) Analyst initiates a remote search in one or more trusted circles in which their company has a membership.
4) Peers in trusted circles initiate local Sighting Search for occurrences of observables in their environment.
5) Peers respond to shared information with their results.

© 2017 ServiceNow All Rights Reserved

Case Management

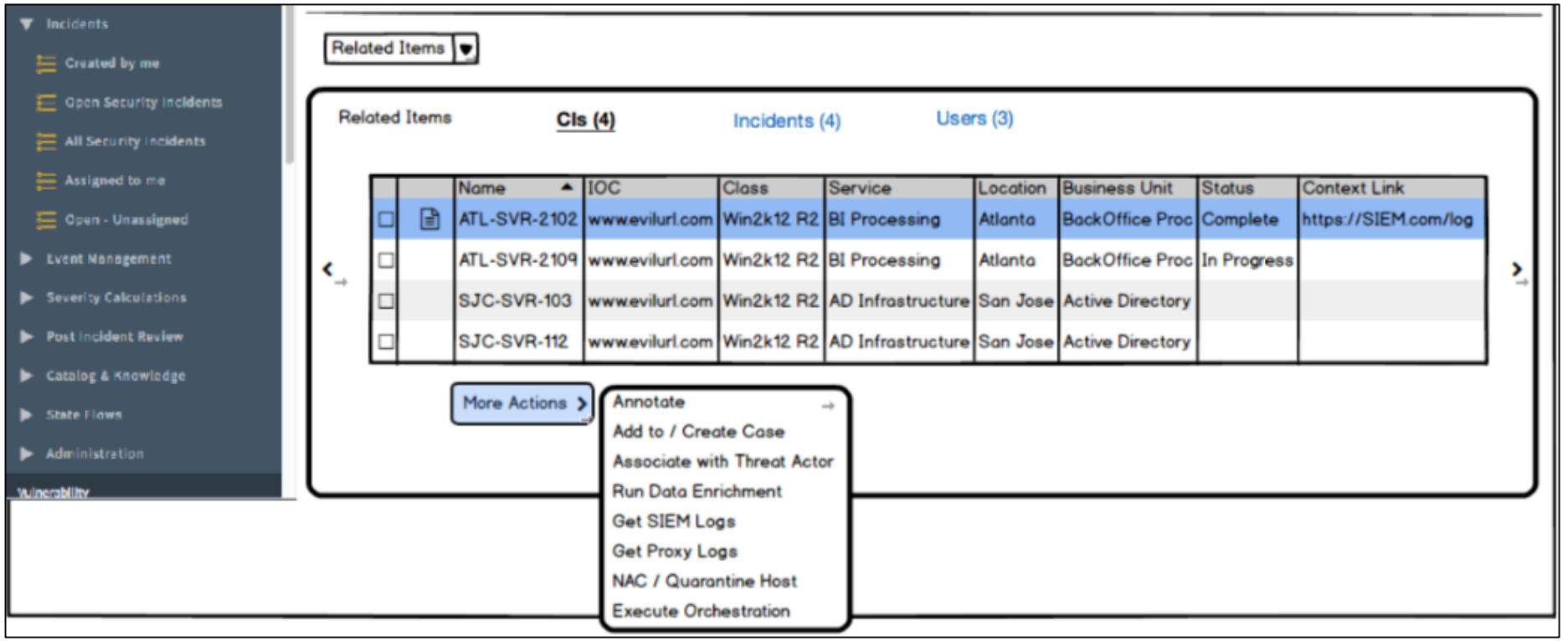


© 2017 ServiceNow All Rights Reserved

IR Action Framework

© 2017 ServiceNow All Rights Reserved

Enable IR Action Framework



Enhanced Data Enrichment

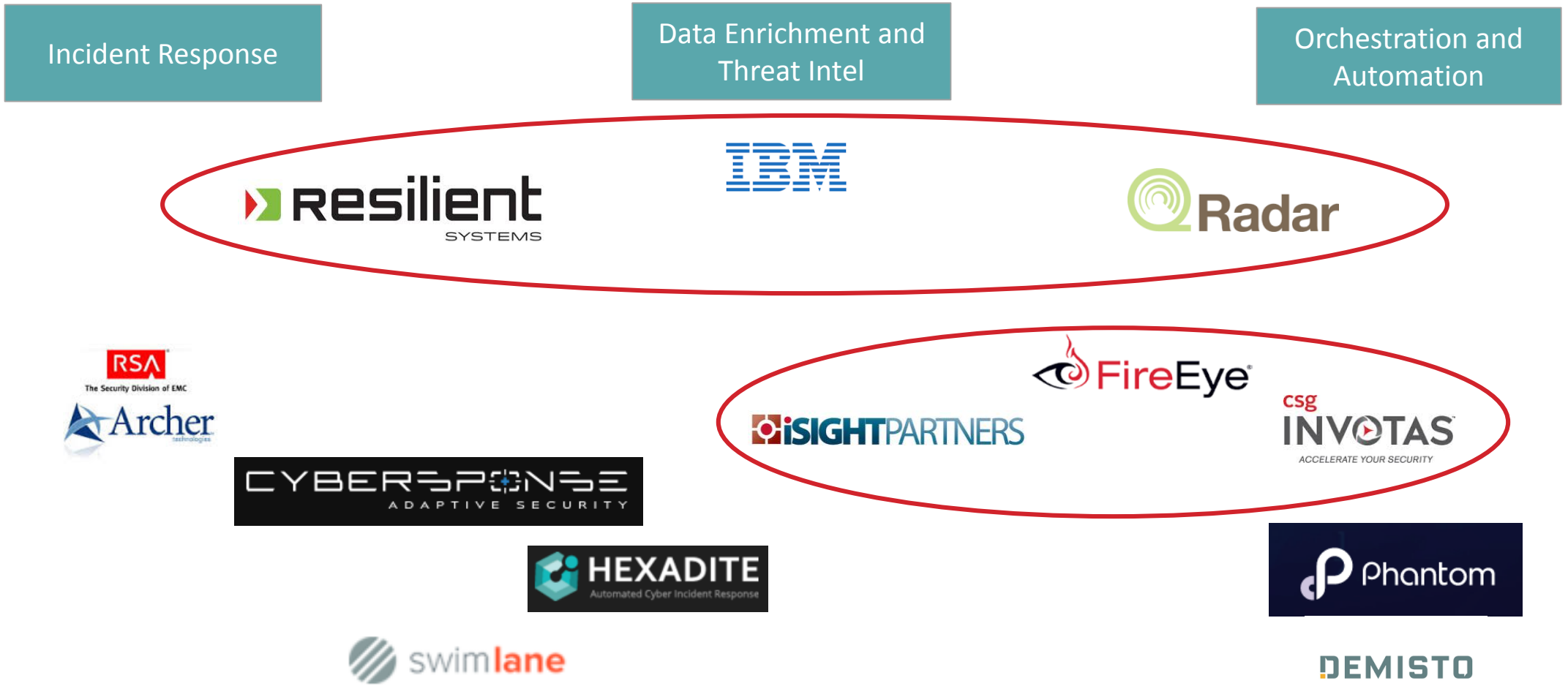
- Process discovery w/ command line argument support
- Service to process mapping
- Child and parent process identification
- Whitelist and blacklisting of enriched data w/ regex support

Updated Action Framework

- Support for Capabilities API
- Ability to invoke any orchestration
- Multi-OS support for process enrichment (Linux / Unix)
- Execute ProcDump for analysis
- WHOIS and reverse IP lookup support
- HaveIBeenP0wned Integration

© 2017 ServiceNow All Rights Reserved

Competitive Overview



Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

Strategic Roadmap

STRATEGIC INITIATIVE	NEAR-TERM	BIG BET
Accelerate customer adoption	Content library	Dynamic runbook
Change the market baseline	Threat intel sharing and threat hunting	Global compute policy enforcement
Innovate and extend	Vendor risk 1.0	Multi-company information sharing and brokering

© 2017 ServiceNow All Rights Reserved

Security Industry Workforce Shortfall

The 2015 (ISC)² Global Information Security Workforce Study

The most recent (ISC)² Global Information Security Workforce Study similarly revealed a workforce gap in the information security field of 1.5 million in the next five years.

Cisco 2014 Annual Security Report Industry

"… the industry will still be short more than a million security professionals across the globe."

peninsula press

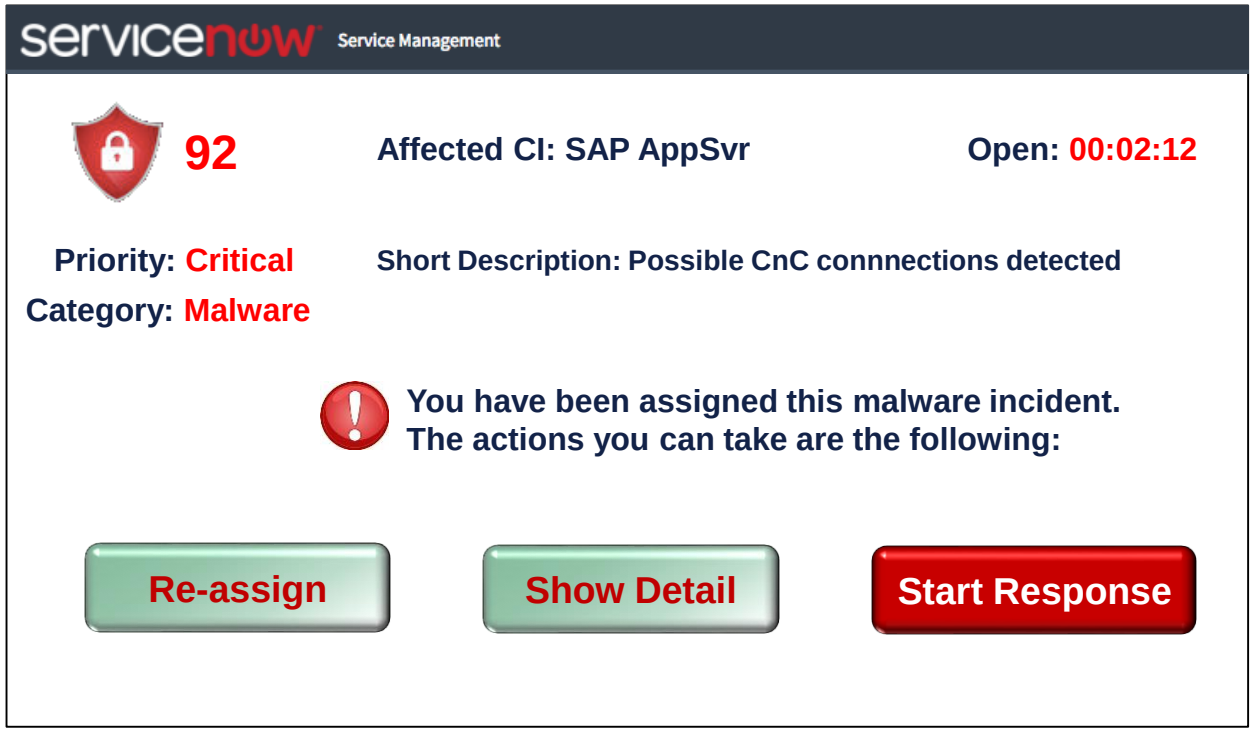
"More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years."

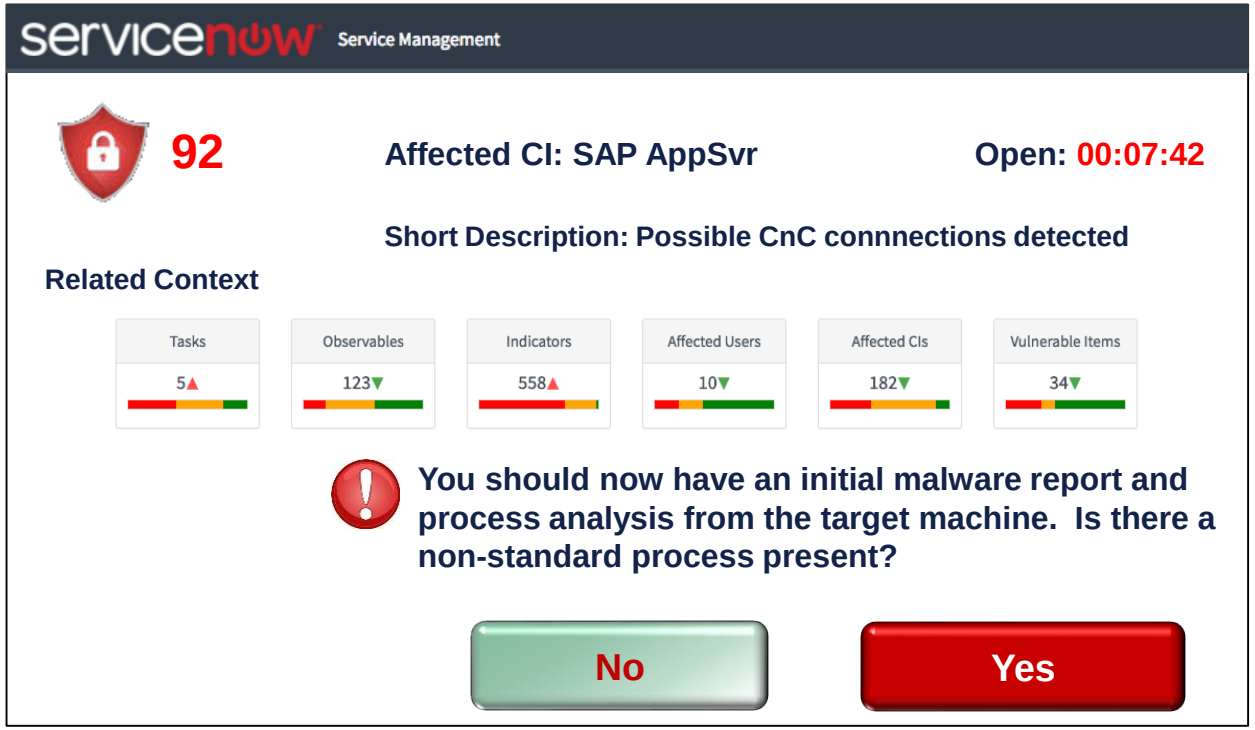
Source: Bureau of Labor Statistics

Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

Dynamic Run-Book





© 2017 ServiceNow All Rights Reserved

GRC Roadmap

© 2017 ServiceNow All Rights Reserved

GRC Roadmap



Jakarta (May ‘17)

Launch Vendor Risk

- Vendor Assessment Workflow
- Vendor Responses to Controls Mapping
- Vendor Tiers and Risk Scoring
- Vendor Portal

Kingston (Dec ’17)

Mature Vendor Risk

- Vendor Exchange – Phase I
- Extensible Content Store

CI Security Posture

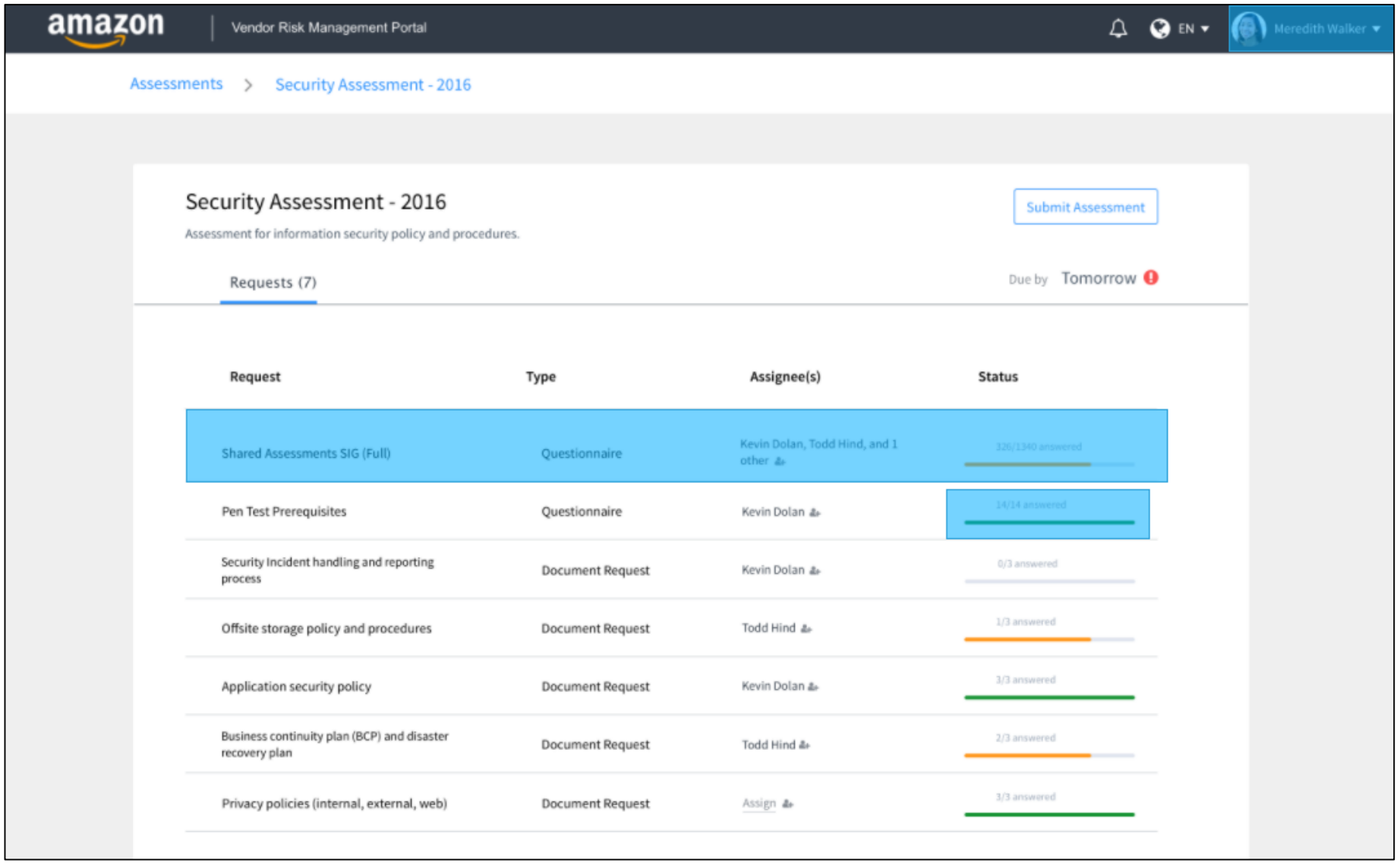
- Crown Jewel Identification
- Control Testing on Target Assets
- Integrations with Configuration Scanners

Threat Risk Mapping

- Threat Adversary Business Impact Mapping
- Threat Adversary Dashboard

© 2017 ServiceNow All Rights Reserved

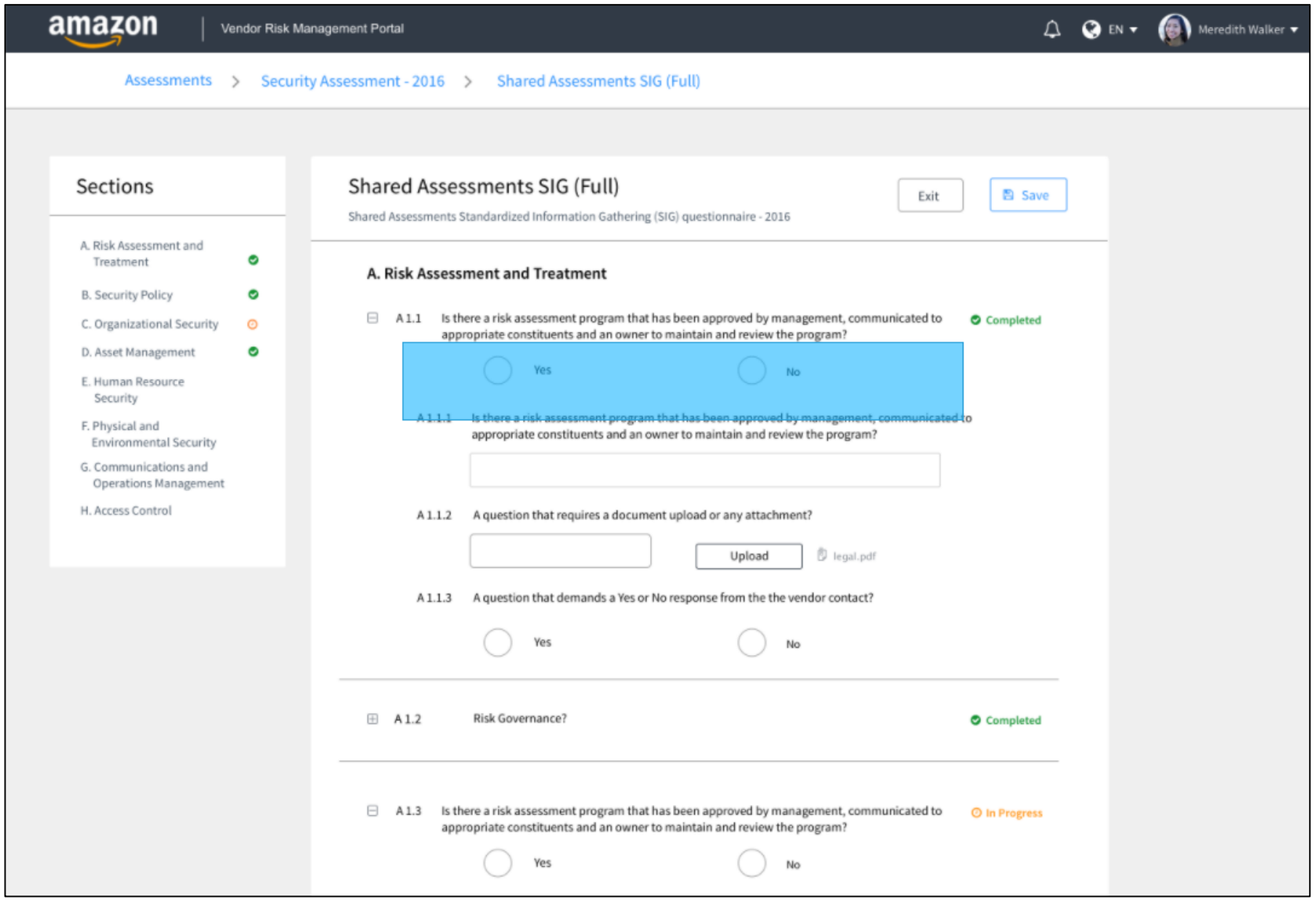
Vendor Assessment Portal



Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

© 2017 ServiceNow All Rights Reserved

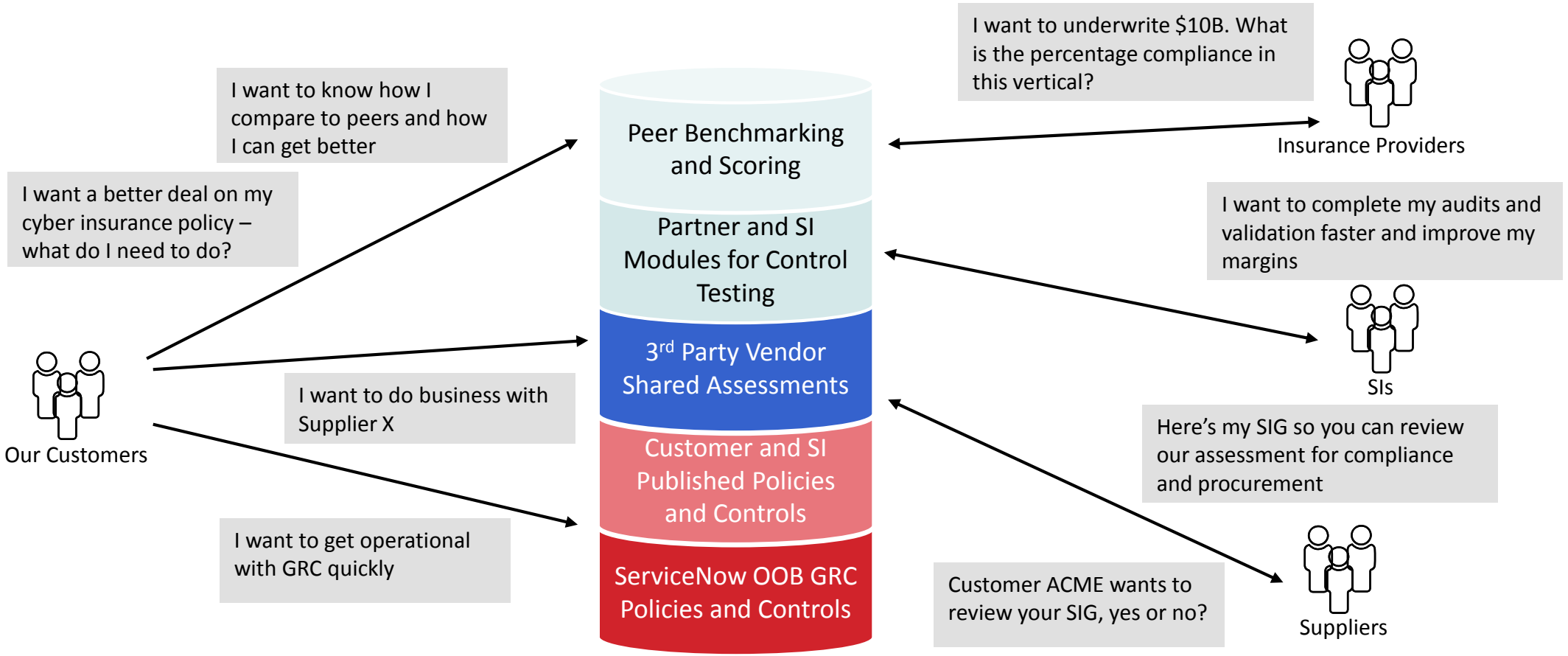
Vendor Assessment Portal



Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow

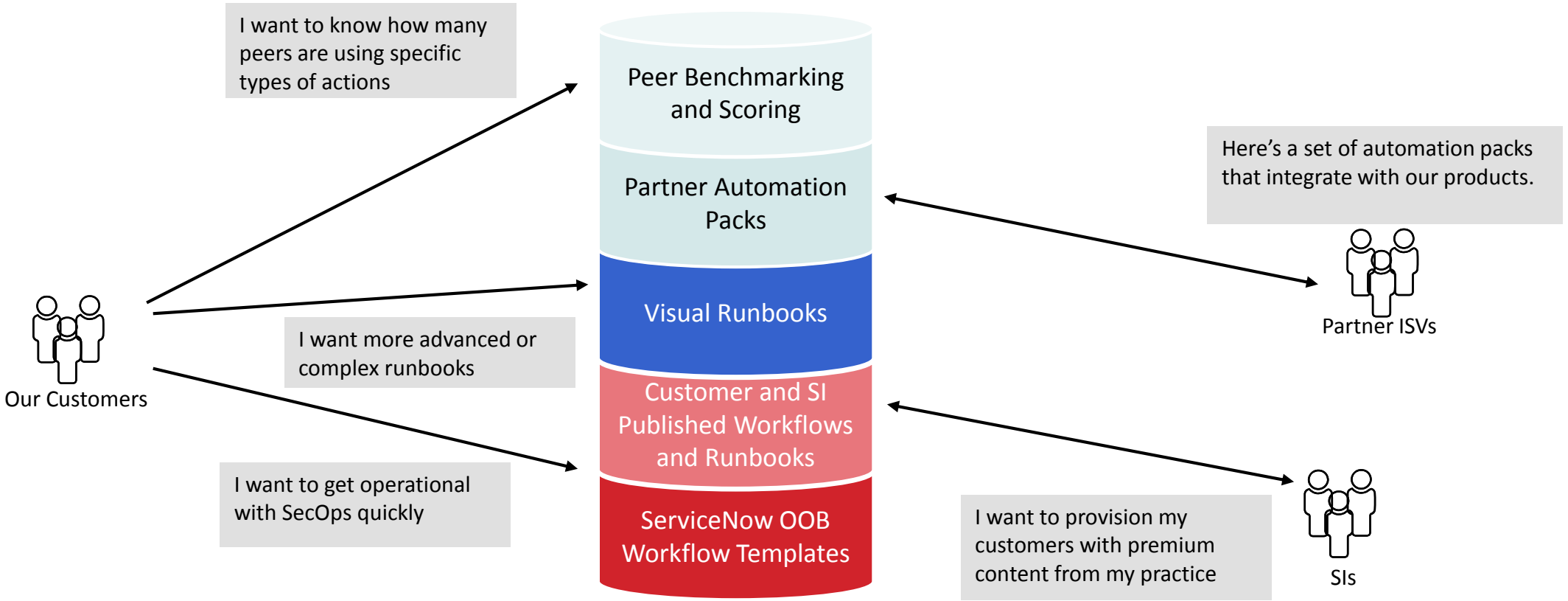
© 2017 ServiceNow All Rights Reserved

The Vision:
A Cloud-based System of Engagement for Risk + Security



© 2017 ServiceNow All Rights Reserved

The Vision:
A Cloud-based System of Engagement for Risk + Security



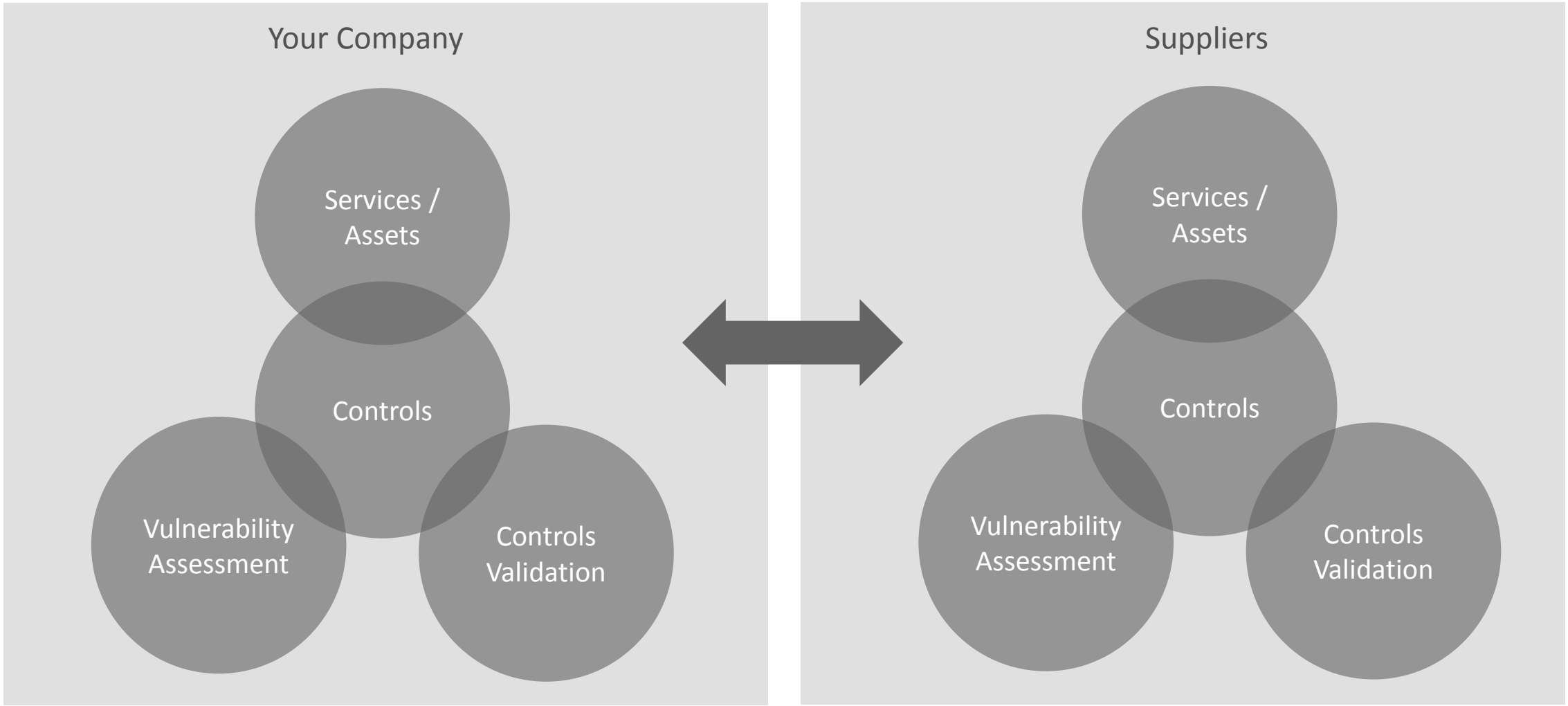
© 2017 ServiceNow All Rights Reserved

Next Gen VR

Vision: ServiceNow Security will know the security posture of every compute asset in the world

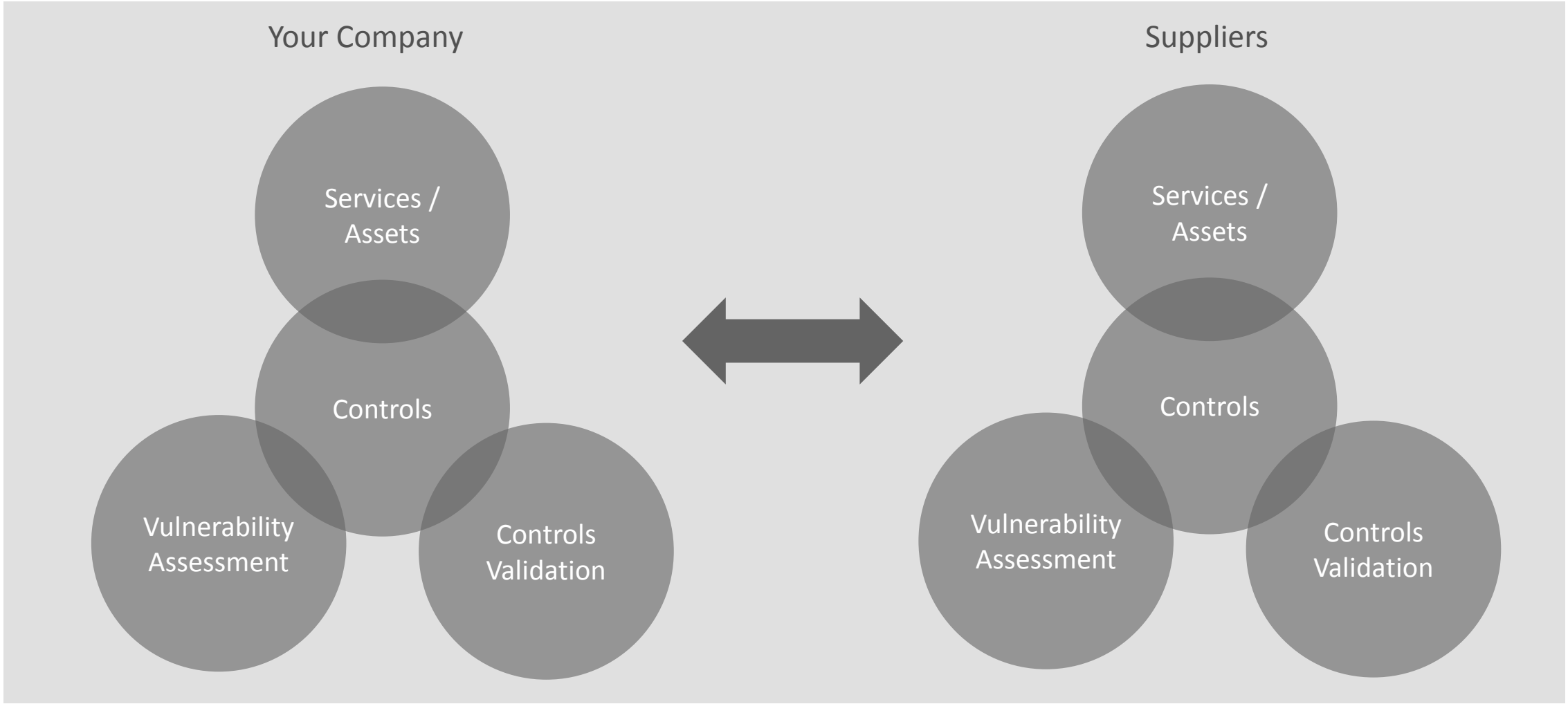
© 2017 ServiceNow All Rights Reserved

Security Posture Convergence – K Release



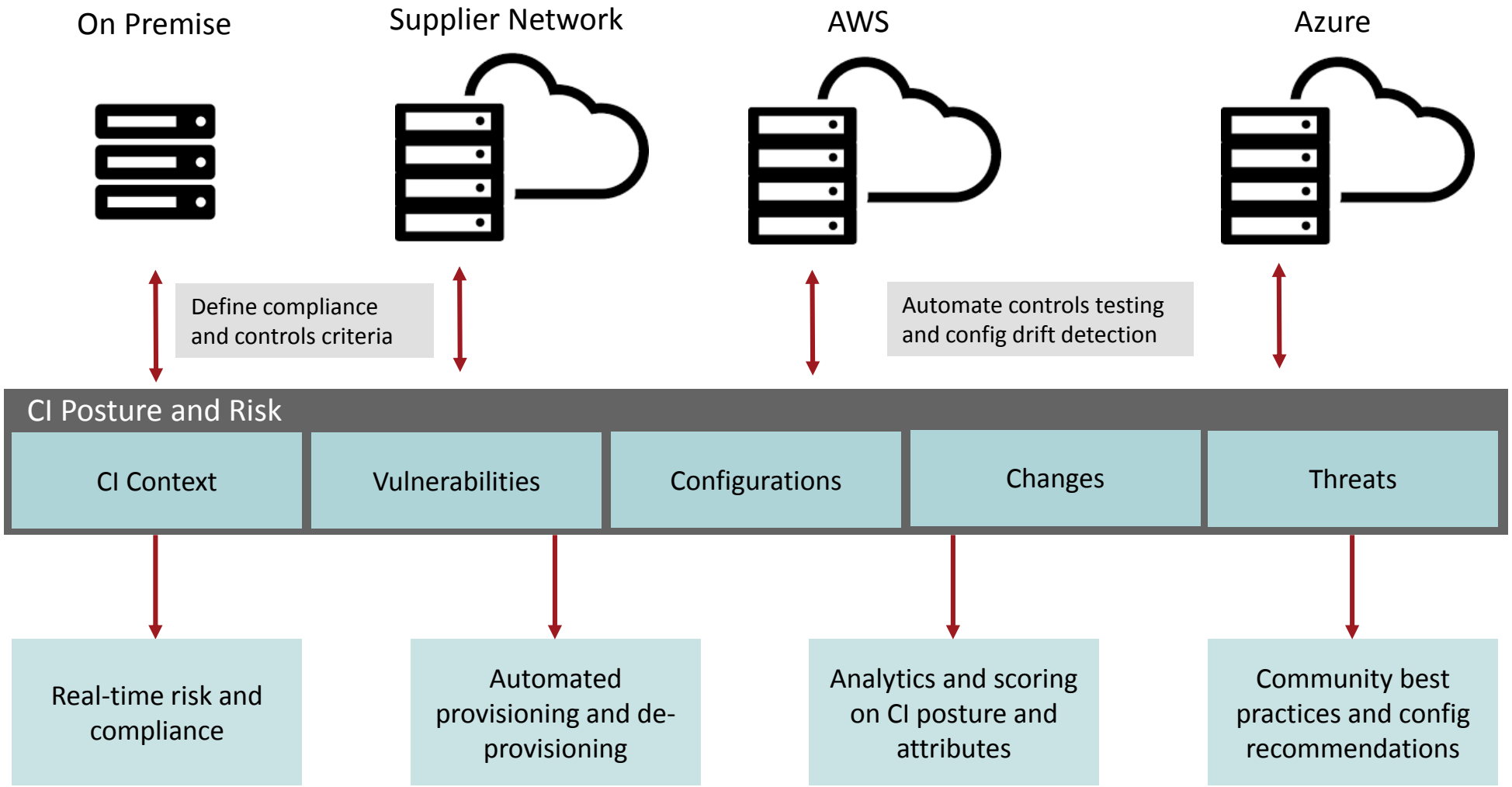
© 2017 ServiceNow All Rights Reserved

Security Posture Convergence – K Release



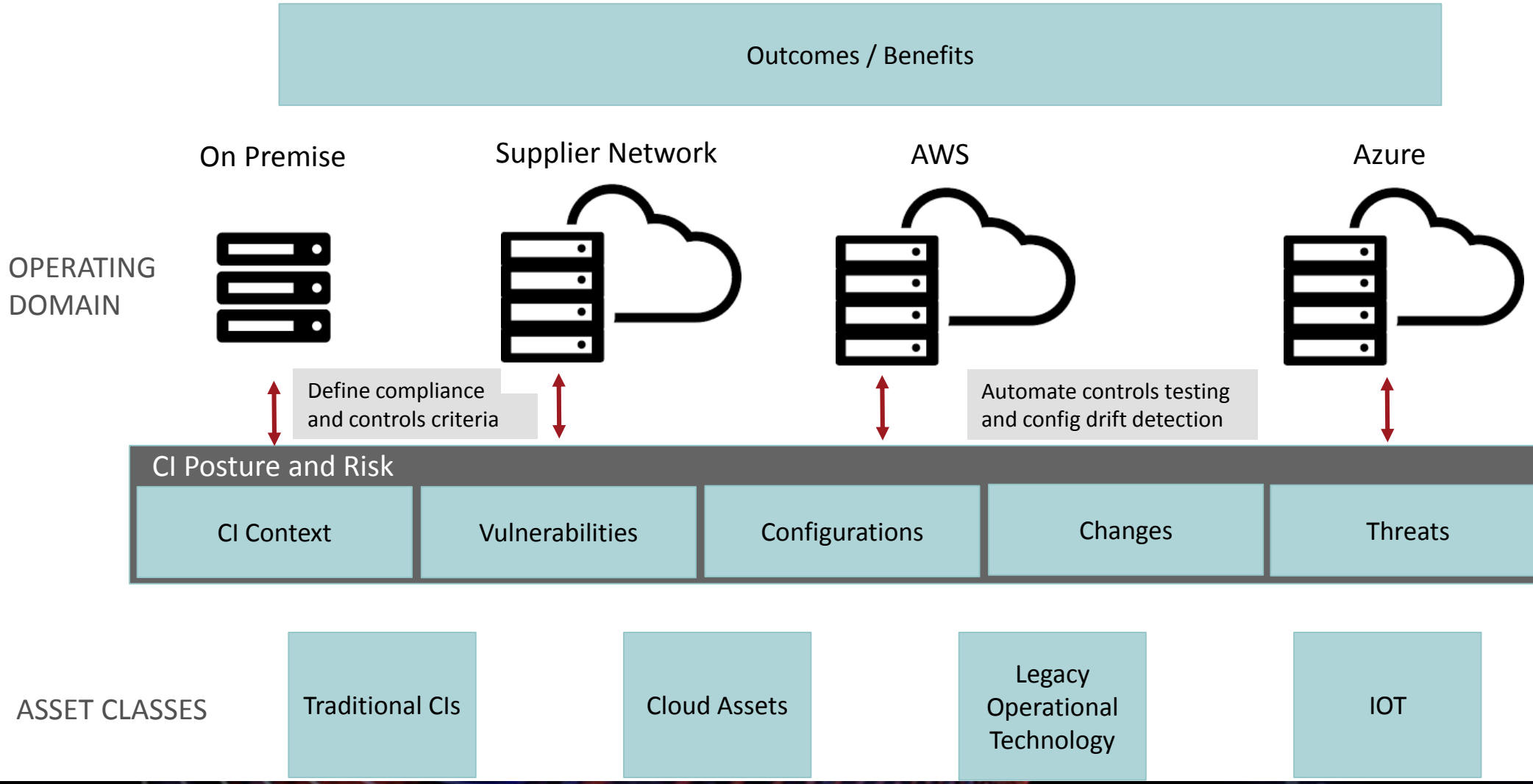
© 2017 ServiceNow All Rights Reserved

Global Compute Policy Enforcement



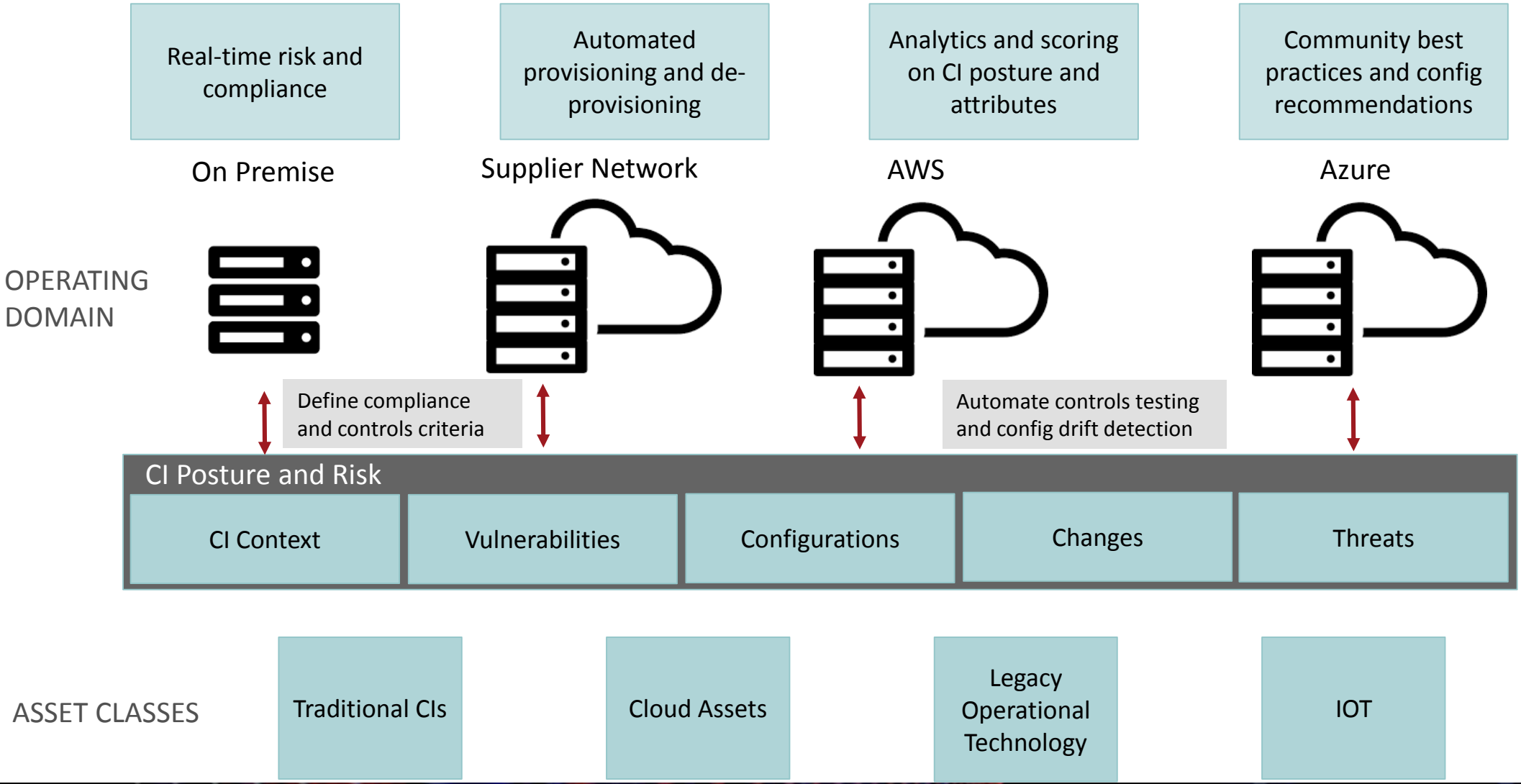
© 2017 ServiceNow All Rights Reserved

Service-Centric Assessment and Control



© 2017 ServiceNow All Rights Reserved

Service-Centric Assessment and Control



© 2017 ServiceNow All Rights Reserved

Q & A

HAROLD BYUN
SR. DIRECTOR, PRODUCT MANAGEMENT
ServiceNow

© 2017 ServiceNow All Rights Reserved

Take the Survey

Please take a moment to complete a session survey in the Knowledge17 app.

Thank You

Harold Byun

Sr. Director, Product Management

ServiceNow

© 2017 ServiceNow All Rights Reserved